Layer 4-Layer 7 Service

• Layer 4-Layer 7 Service, on page 1

Layer 4-Layer 7 Service

Cisco DCNM Release 11.3(1) introduces the ability to insert Layer 4-Layer 7 (L4-L7) service devices in a data center fabric, and also enables selectively redirecting traffic to these service devices. You can add a service node, create route peering between the service node and the service leaf switch, and then selectively redirect traffic to these service nodes.

You can also watch a video that demonstrates how to orchestrate a L4-L7 Service Appliance with a VXLAN Fabric in a data center managed by Cisco DCNM. This demo covers provisioning, defining of service policies, and monitoring of redirected flows. For information, see Video: Service Redirection in Cisco DCNM.

Service Node

You have to create an external fabric and specify that a service node resides in that external fabric during service node creation. DCNM does not auto-detect or discover any service node. You also have to specify the service node name, type, and form factor. The name of the service node has to be unique within a fabric. The service node is attached to a leaf, border leaf, border spine, or a border super spine. Starting from Cisco DCNM Release 11.4(1), the service node can be attached to a vPC border gateway also. DCNM does not define a new switch role for a service leaf.

DCNM manages the switches that are attached to a service node. DCNM also manages the interfaces of these attached switches. Ensure that the interfaces to which the service node is attached to are in trunk mode and do not belong to any interface group. The L4-L7 service will not change its mode. In case the attached switches are forming a vPC pair, the name of the attached switch is a combination of both switches.

Route Peering

Route peering creates service networks. DCNM supports both static route and eBGP-based dynamic route peering options. After you specify the service network and select the peering policy for the tenant, DCNM automatically creates the service network under the specified tenant. Note that the terms, tenant and VRF, will be used interchangeably in this guide. If you select a route peering and click **Deploy** in the **Service Nodes** window, the L4-L7 service deploys the corresponding service network and VRF configuration to the leaf that is attached to the service node. Click **Preview** to review both the peering and service network configuration.

The automatically created service network will also be listed on the **Control > Fabrics > Networks** window. You can view and edit the corresponding config parameters in the **Networks** window. However, you cannot

Layer 4-Layer 7 Service

delete the service network. Deletion of service networks is handled automatically during the service route peering deletion process. There can be multiple route peerings defined per tenant/VRF.

Service Policy

You can only define the service policy between the created networks. The L4-L7 service does not create any VRF or network other than the service networks that are defined during route peering. The source and destination network can be a subnet, an individual IP address or the networks that are defined in the **Control > Fabrics > Networks** window. Note that the source or destination network can also be defined by using the **any** CLI keyword. This means that any IP address traffic is supported. For intra-tenant firewall, one-arm and two-arm load balancer, the L4-L7 service in DCNM uses Policy-Based Routing (PBR) for service insertion. The inter-tenant firewall does not have a service policy. You only need to create a service node and route peering for inter-tenant firewall.

As the source and destination network can be attached or deployed independent of service policy deployment, the tenant/ VRF-related service policy configuration is only attached or pushed to the switch that is attached to the service node, and the source and destination network is updated with the service policy-related configuration. You can preview and confirm the generated configuration. By default, the service policy is defined but is not enabled or attached. You have to enable or attach the service policy to activate it.

The service configuration that is related to the source and destination network will be auto-processed when the source and destination networks are to be attached, or auto-updated in case the networks are already attached or deployed. By default, DCNM will collect statistics every 5 minutes and store it in ElasticSearch for aggregation and analysis. Click the graph line under **Stats** in the **Service Policy** tab of the **Service Nodes** window to view the historical time-based statistics. By default, the statistics are stored for a maximum of 7 days.

The service insertion is effective only on the flows to be created. There is no impact on any existing flows. Deletion of a network is not allowed in case an enabled service policy is associated with that network.

The L4-L7 service integration is built on top of the easy fabric policy enforcement. Use the fabric builder to create a VXLAN EVPN fabric and then import Cisco Nexus 9000 Series switches into the fabric with pre-defined fabric policies.

MSD Support

Starting from Cisco DCNM Release 11.4(1), this feature supports Multi-Site Domains (MSD). Select the MSD member fabric from the DCNM fabric scope selector, create a service node (for example, firewall, or load balancer), attach the service node to the switch in the selected MSD member fabric, define the route peering and service policies, and deploy relevant configurations on the selected MSD member fabric. For more information on the procedure to configure Layer 4-Layer 7 service, refer Configuring Layer 4-Layer 7 Service, on page 7.

RBAC Support

Starting from Cisco DCNM Release 11.4(1), the Layer 4-Layer 7 Service supports Role-Based Access Control (RBAC) along with fabric access mode.

The admin, stager, and operator, are pre-defined roles in DCNM. The table given below lists the various operations that each role can perform.

L4-L7 Service Operation	Service Node	Route Peering	Service Policy
Create/Update/Delete/Import	admin	admin, stager	admin, stager

Layer 4-Layer 7 Service

L4-L7 Service Operation	Service Node	Route Peering	Service Policy
List/Export	admin, stager, operator	admin, stager, operator	admin, stager, operator
Attach/Detach	NA	admin, stager	admin, stager
Deploy	NA	admin (blocked if fabric is in fabric monitor or read-only mode)	admin (blocked if fabric is in fabric monitor or read-only mode)
Preview/Deployment History	NA	admin, stager, operator	admin, stager, operator

Note If a fabric is in fabric monitor or read-only mode, an admin cannot deploy the route peering or service policy. Also, the icon to delete the service node is not displayed if the external fabric where the service node is located is in fabric Monitor Mode. Remove the fabric from the fabric Monitor Mode to display the icon to delete the service node. This icon will be shown only to users with admin role access.

The Layer 4-Layer 7 Service windows are displayed based on the logged-in user's role and reflect the actions that the user is allowed to perform. Example screenshots of the Service Nodes window for an admin, stager, and operator role are as given below:

Figure 1: Admin role

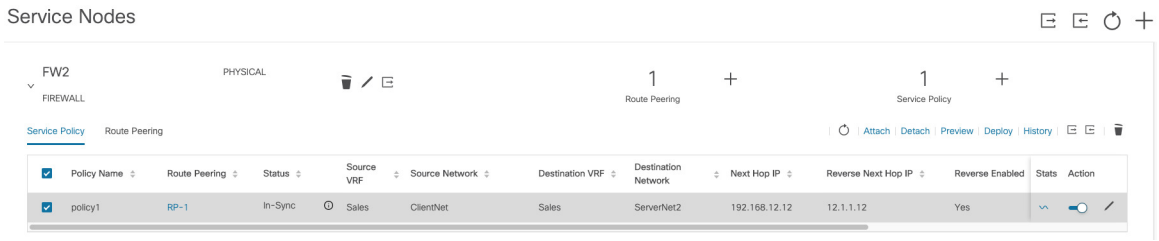


Figure 2: Stager role

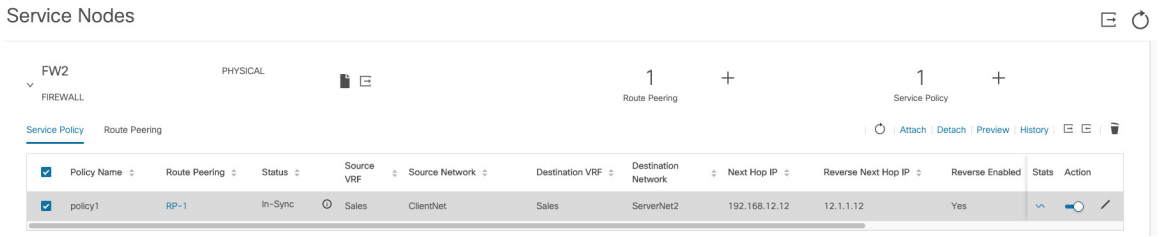
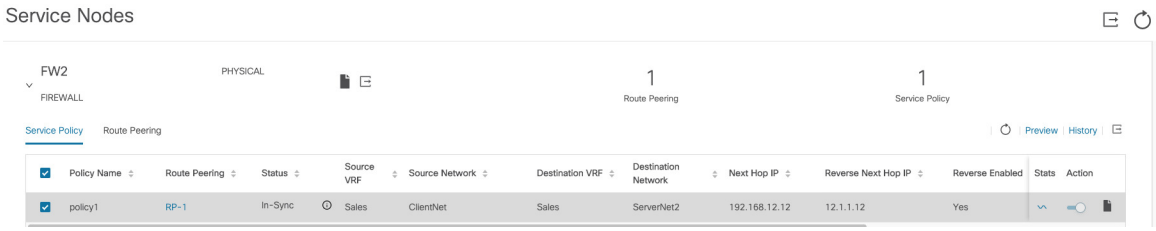


Figure 3: Operator role



Guidelines and Limitations for Layer 4-Layer 7 Service

- L4-L7 service in DCNM does not manage or provision service nodes, such as firewall and load balancer.
- The L4-L7 service feature is supported only on the VXLAN BGP EVPN fabrics with the **Easy_Fabric_11_1** template.
- The service policies defined in this feature leverage Policy-Based Routing (PBR). Refer Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for PBR related configuration, constraints, and so on.
- This feature supports Cisco Nexus 9300-EX and 9300-FX platform switches as leaf, border leaf, border spine, border super spine, and border gateway switches.
- Configurations involving intra-tenant and inter-tenant firewall for L3 networks, and one-arm and two-arm deployed load balancers, are supported.
- The existing DCNM topology view is also leveraged to display redirected flows associated with the switches that the service node is attached to, and to locate specific redirected flows.
- Load sharing is not supported.
- This feature creates, updates, and deletes the service network, as required. Service networks cannot be created or deleted from the **Control > Fabrics > Networks** window.

Types of Layer 4–Layer 7 Service Devices

The L4-L7 service in Cisco DCNM supports any vendors service node attachments. Typical service node types that are deployed in a data center are Firewalls, Load Balancers, and other Layer-4 to Layer-7 products.

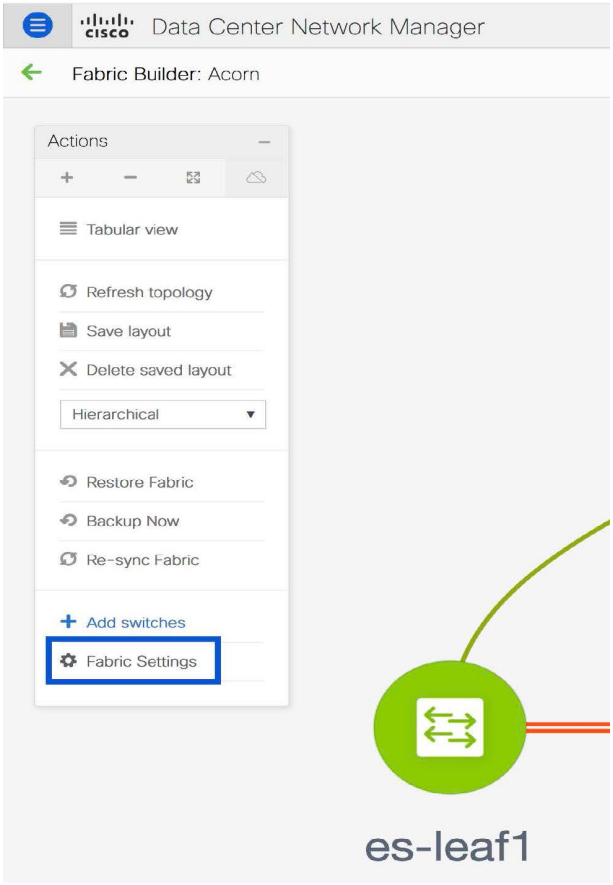
Examples of supported Firewall vendors are Cisco Systems, Palo Alto Networks, Fortinet, Check Point Software Technologies, and others.

Examples of supported Load Balancer vendors are F5 Networks, Citrix Systems, A10 Networks, and others.

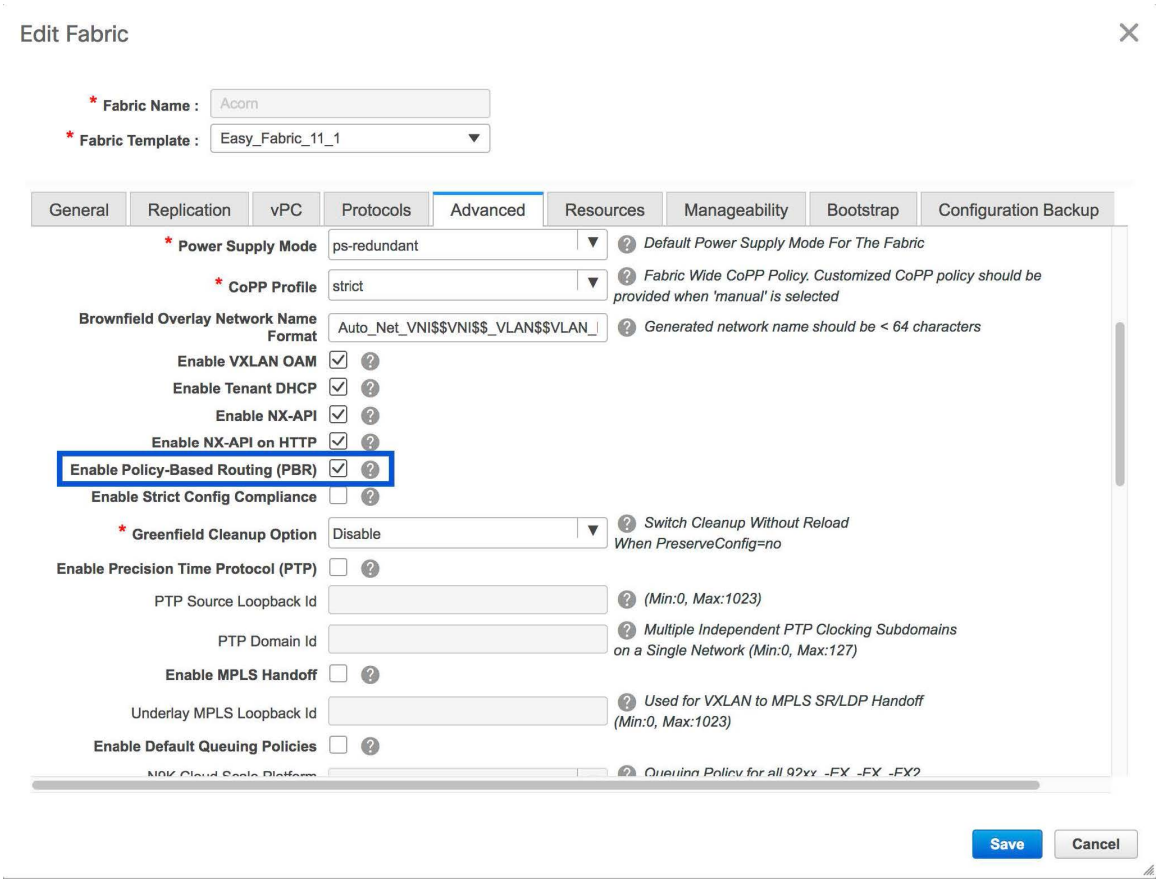
Note that these example lists are meant to serve as examples and not intended to be **exhaustive** lists. The L4-L7 service attachment is generic and applies to any vendors service node.

Configuring Fabric Settings for Layer 4-Layer 7 Service

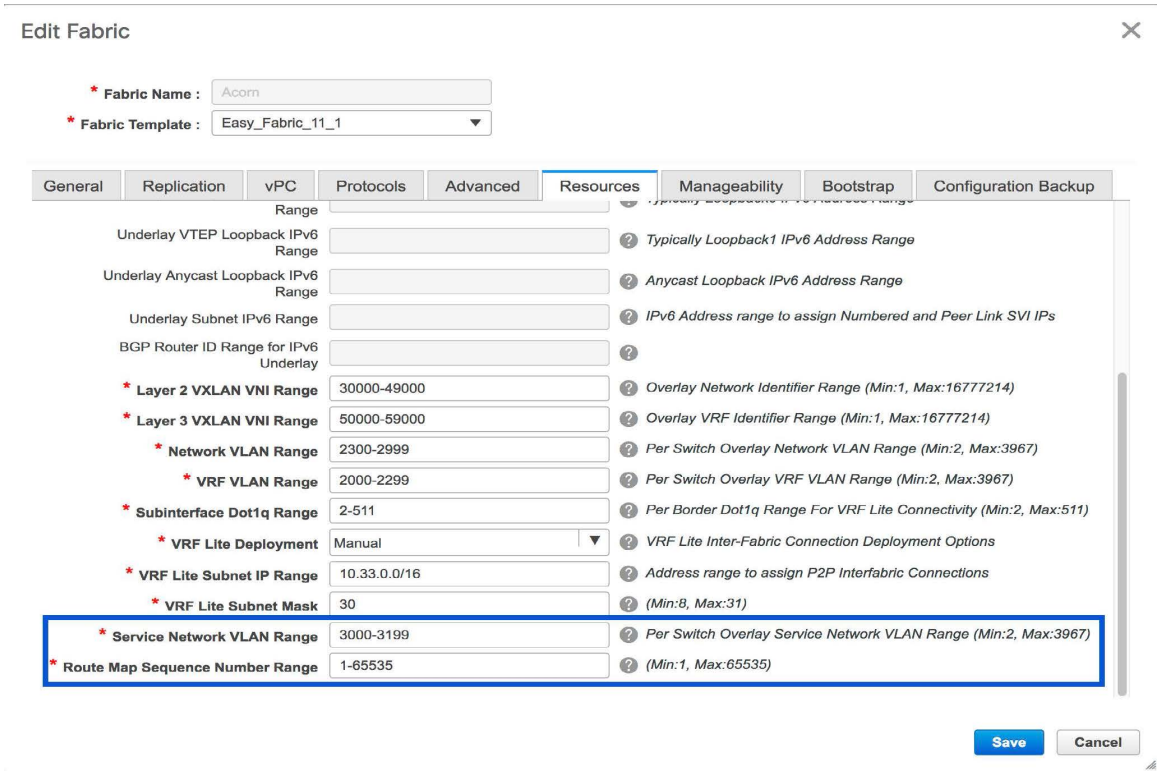
Certain fabric settings have to be configured to enable L4-L7 service functionality. To configure these settings, click **Fabric Settings** under **Actions** in the **Fabric Builder** window.



The **Edit Fabric** window is displayed. Click **Advanced**. Select the **Enable Policy-Based Routing (PBR)** checkbox to enable routing of packets based on the specified policy.



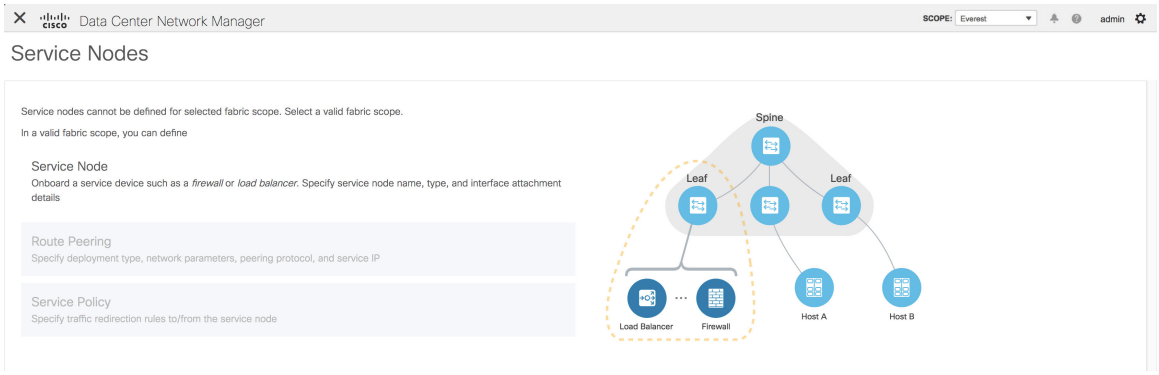
Now, click **Resources**. Specify a VLAN range in the **Service Network VLAN Range** field. This is a per switch overlay service network VLAN range. The minimum allowed value is 2 and the maximum allowed value is 3967. Also, specify a value for the **Route Map Sequence Number Range** field. The minimum allowed value is 1 and the maximum allowed value is 65535. Click **Save and Deploy** to deploy the updated configuration.



Configuring Layer 4-Layer 7 Service

To launch the L4-L7 Service, or the Elastic Service, on the Cisco DCNM Web UI, choose **Control>Fabrics>Services**.

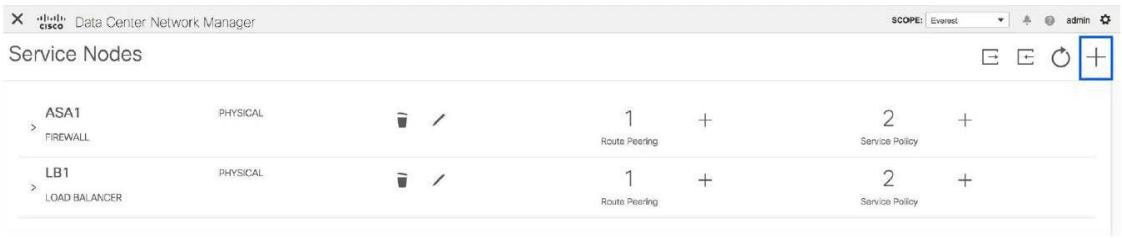
The **Service Nodes** window is displayed. Select a valid switch fabric to display or define the service nodes, route peerings, and service policies, in that fabric.



The L4-L7 service configuration procedure consists of the following steps:

Create Service Node

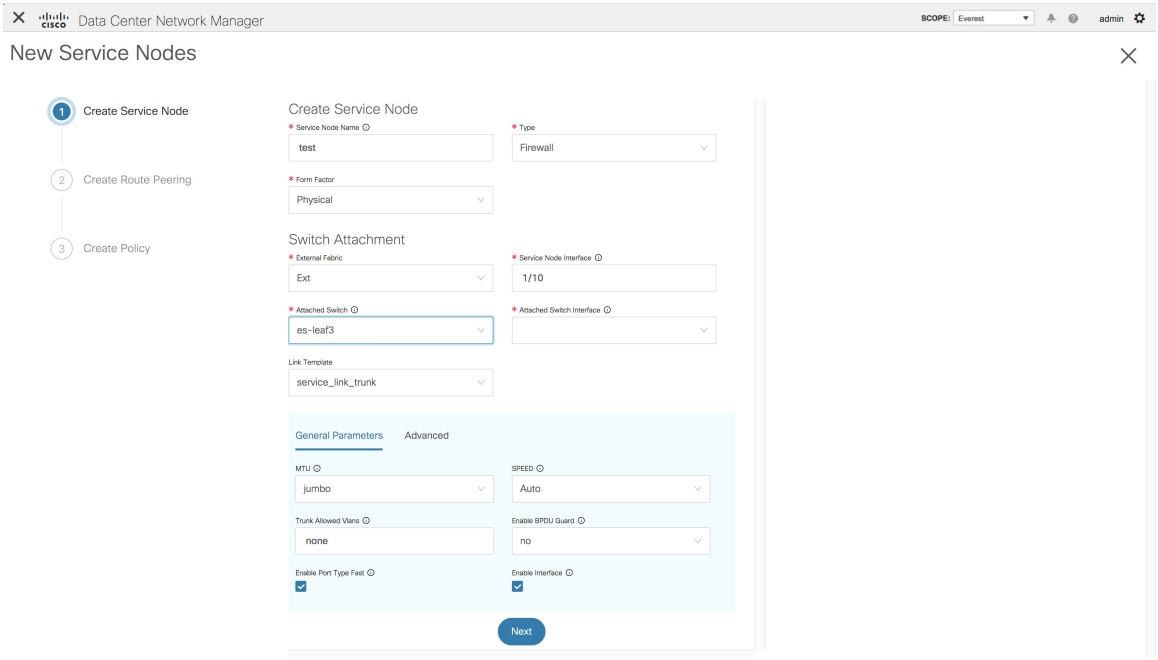
To create a service node, click the + icon at the top right of the **Service Nodes** window to display the **New Service Nodes** window.



The **New Service Nodes** window has three steps, **Create Service Node, Create Route Peering** and **Create Service Policy**.

The **Create Service Node** window has two sections - Create Service Node and Switch Attachment, followed by a **Link Template** drop-down list. You can select service_link_trunk, service_link_port_channel_trunk and service_link_vpc from this drop-down list..

Figure 4: Example: Link Template - service_link_trunk



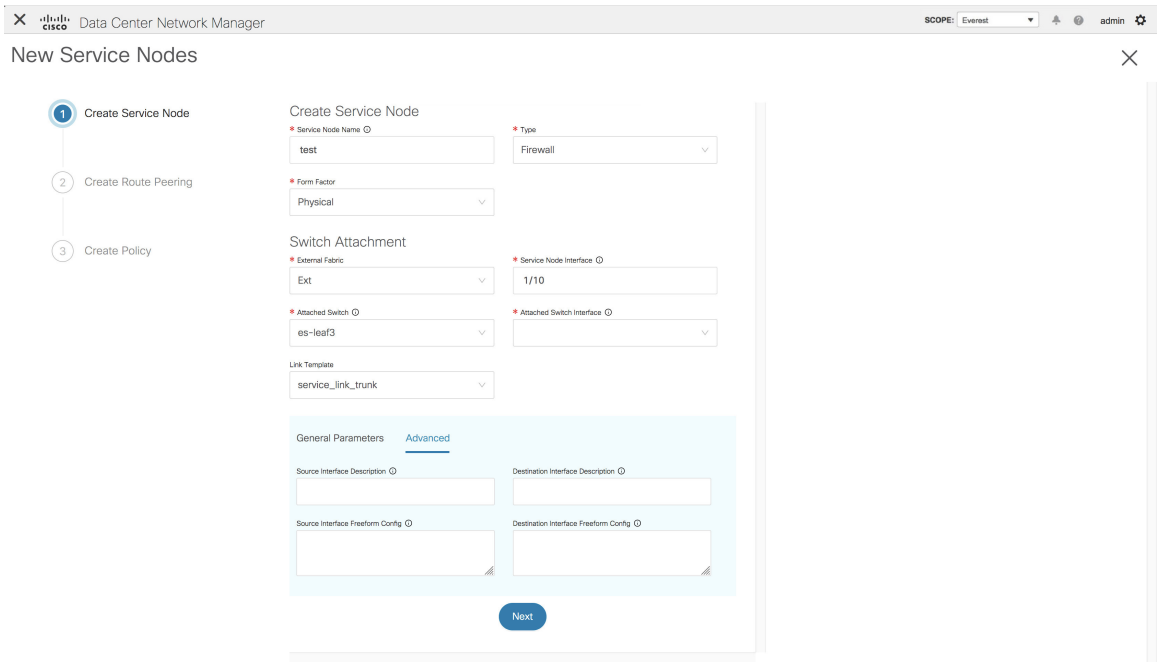


Figure 5: Example: Link Template - service_link_port_channel_trunk

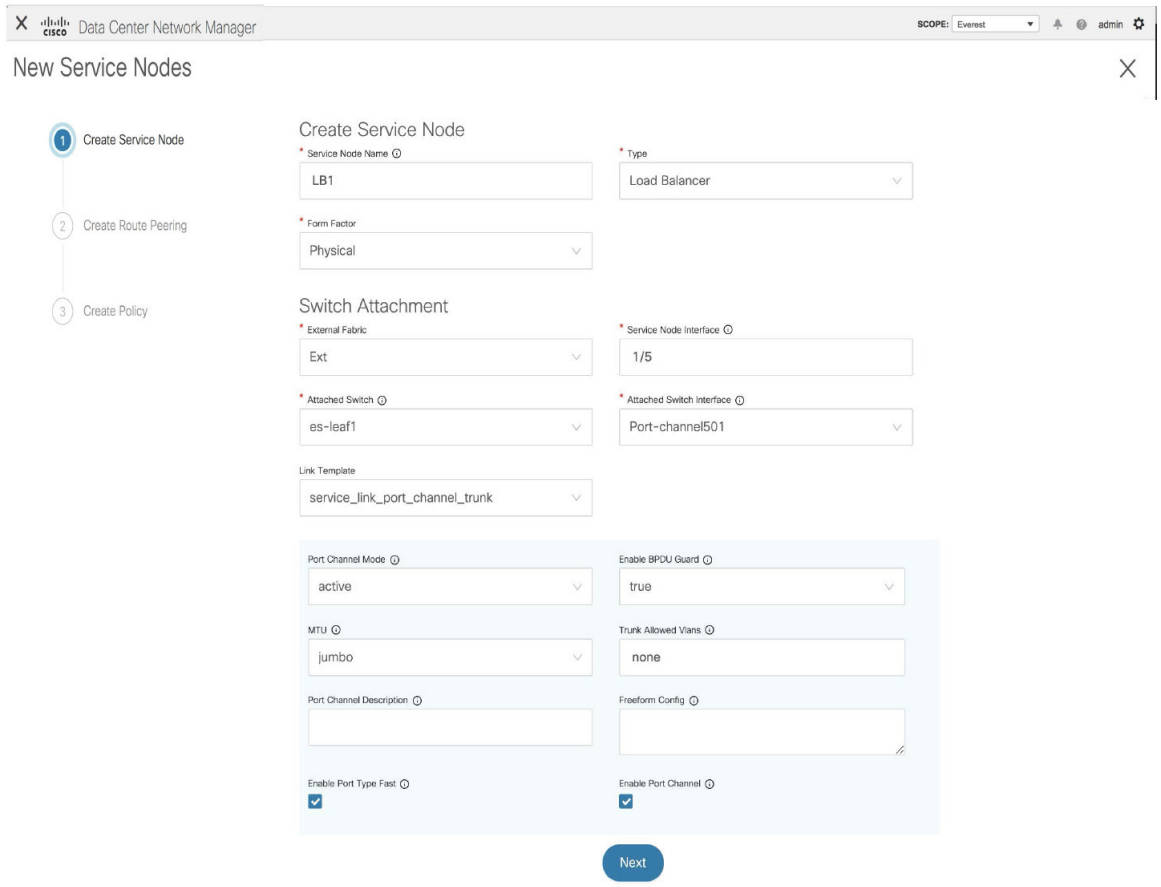
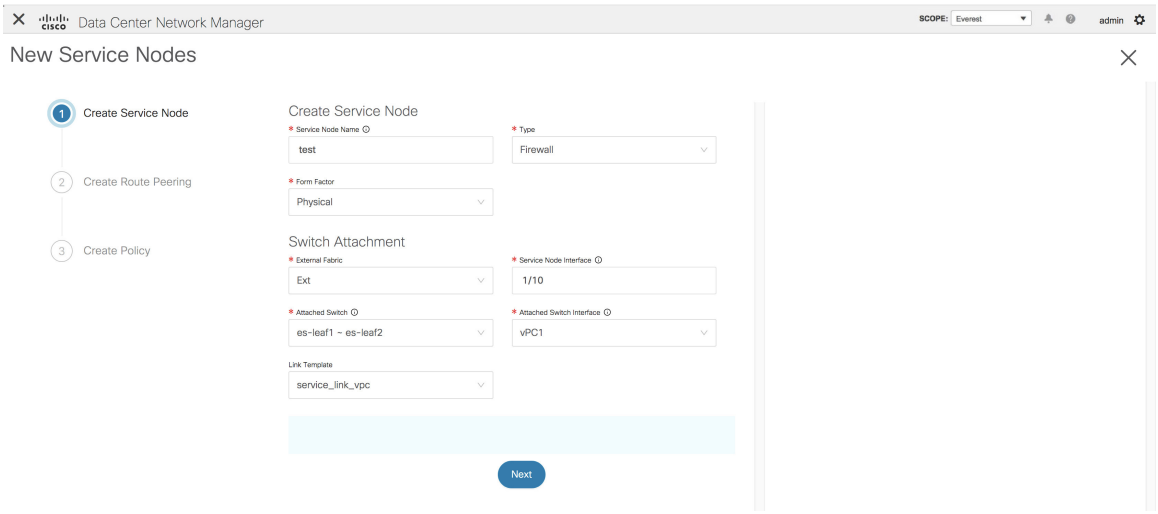


Figure 6: Example: Link Template - service_link_vpc



The fields in the **Create Service Node** window are as given below. It is mandatory to fill the fields marked with an asterisk. For more information on the fields in this window, hover over the **i** icon.

Create Service Node

Service Node Name - Enter a name for the service node. The name can have alphanumeric, underscore, or dash characters.

Type - Select Firewall or Load Balancer.

Form Factor - Select Physical or Virtual.

Switch Attachment

External Fabric - Specify the external fabric.

Service Node Interface - Specify the service node interface.

Attached Switch- Select a switch from the drop-down list.

Attached Switch Interface - Select the interface from the drop-down list. In case the vPC pair is selected from the **Attached Leaf Switch** drop-down list, the vPC channel will be shown in the **Attached Leaf Switch Interface** drop-down list. Otherwise, the port-channel and interfaces with trunk mode are shown in the **Attached Leaf Switch Interface** drop-down list.

Link Template - Select the service_link_trunk, service_link_port_channel_trunk, or the service_link_vpc template. For more information on template fields, refer Templates.

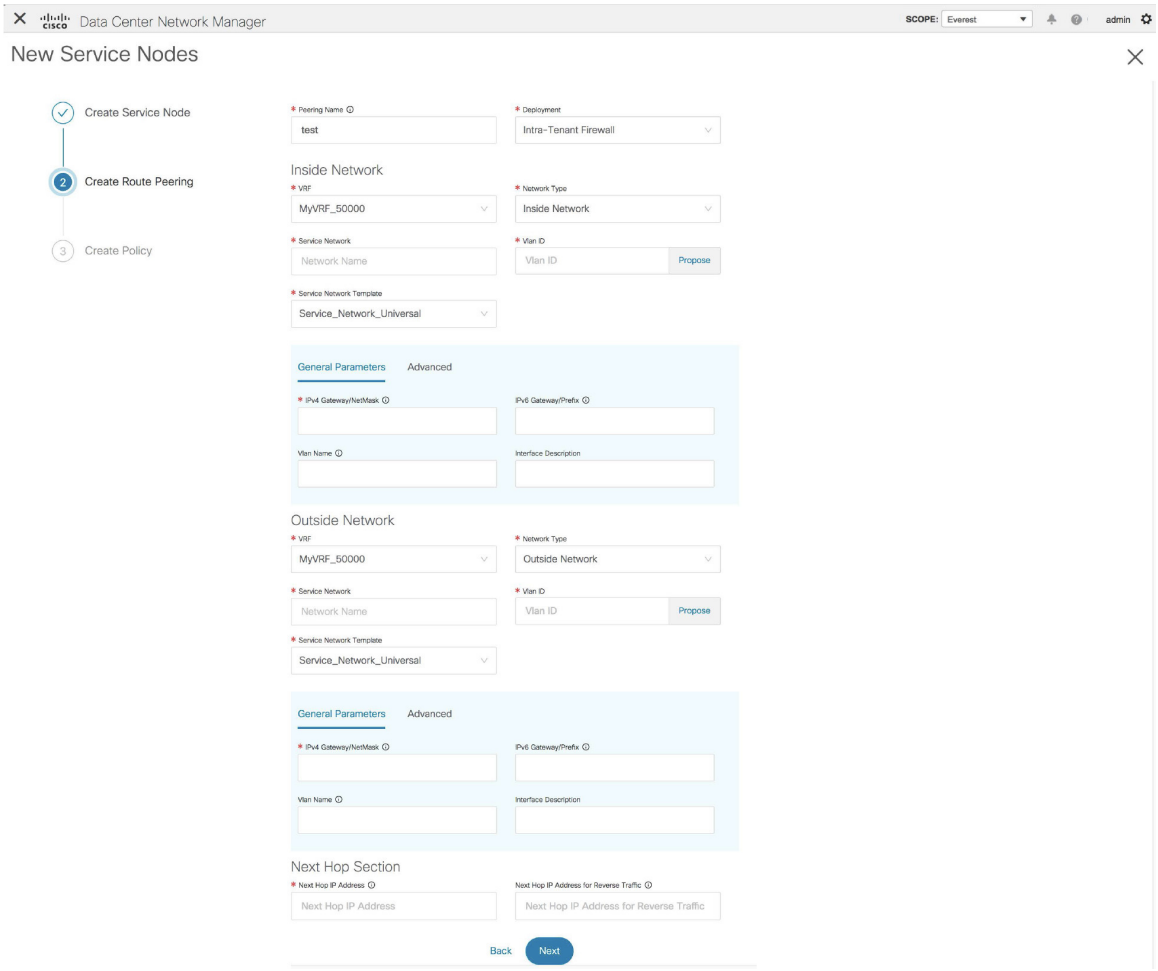
Now, click **Next**. A pop-up window is displayed stating that a new service node has been created successfully and the **Create Route Peering** window is displayed.

Create Route Peering

The fields that appear in the **Create Route Peering** window depend on the type of deployment chosen in the **Create Service Node** window. Depending on the type chosen (Firewall or Load Balancer), the types of deployments are Intra-Tenant Firewall, Inter-Tenant Firewall, One-Arm load balancer and Two-Arm load balancer.

Note Deletion of service network is not supported in Top-down provisioning.

Example: Intra-Tenant Firewall Deployment



The fields in the **Create Route Peering** window for an Intra-Tenant Firewall deployment are as given below. It is mandatory to fill the fields marked with an asterisk. For more information on the fields in this window, hover over the **i** icon.

Peering Name - Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment - Select Intra-Tenant Firewall.

Inside Network

VRF - Specify the VRF.

Network Type - Select Inside Network.

Service Network - Specify the name of the service network.

Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click Propose to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

Outside Network

VRF - Specify the VRF.

Network Type - Select Outside Network.

Service Network - Specify the name of the service network.

Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click Propose to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

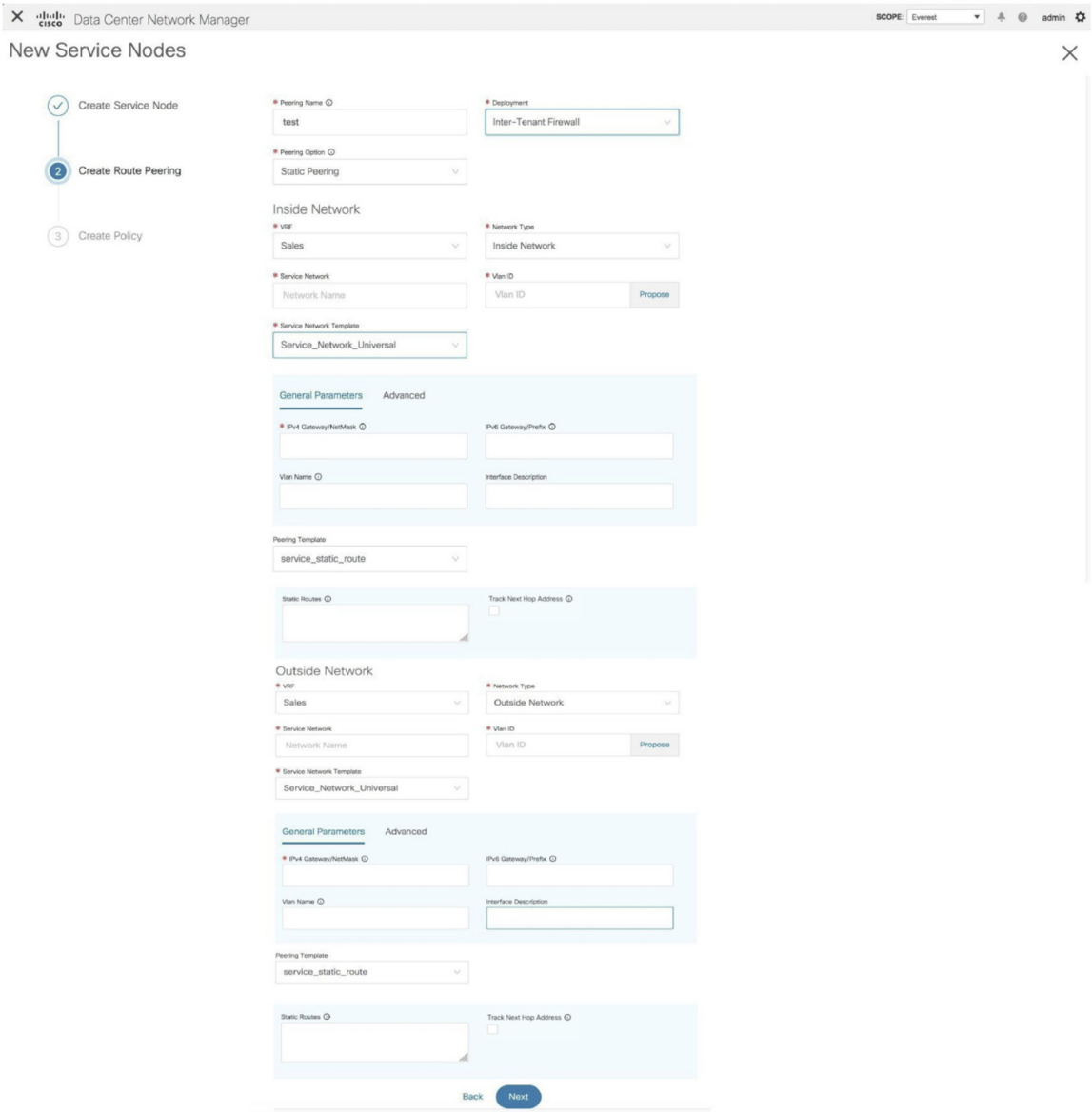
Next Hop Section

Next Hop IP Address - Specify the next-hop IP address. This is the IP/VIP of the service node used for traffic redirection.

Next Hop IP Address for Reverse Traffic - Specify the next-hop IP address for reverse traffic. This is the IP/VIP of the service node used for traffic redirection.

Example: Inter-Tenant Firewall Deployment

Peering Option - Static Peering, Inside Network Peering Template - service_static_route, Outside Network Peering Template - service_static_route



The fields in the **Create Route Peering** window for an Inter-Tenant Firewall deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

Peering Name - Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment - Select Inter-Tenant Firewall.

Peering Option - Select Static Peering or eBGP Dynamic Peering.

Inside Network

VRF - Select a VRF from the drop-down list..

Network Type - Select Inside Network.

Service Network - Select a service network name from the drop-down list.

Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

Peering Template - Select service_static_route or service_ebgp_route from the drop-down list. For more information on the template fields, refer Templates.

Outside Network

VRF - Select a VRF from the drop-down list..

Network Type - Select Outside Network.

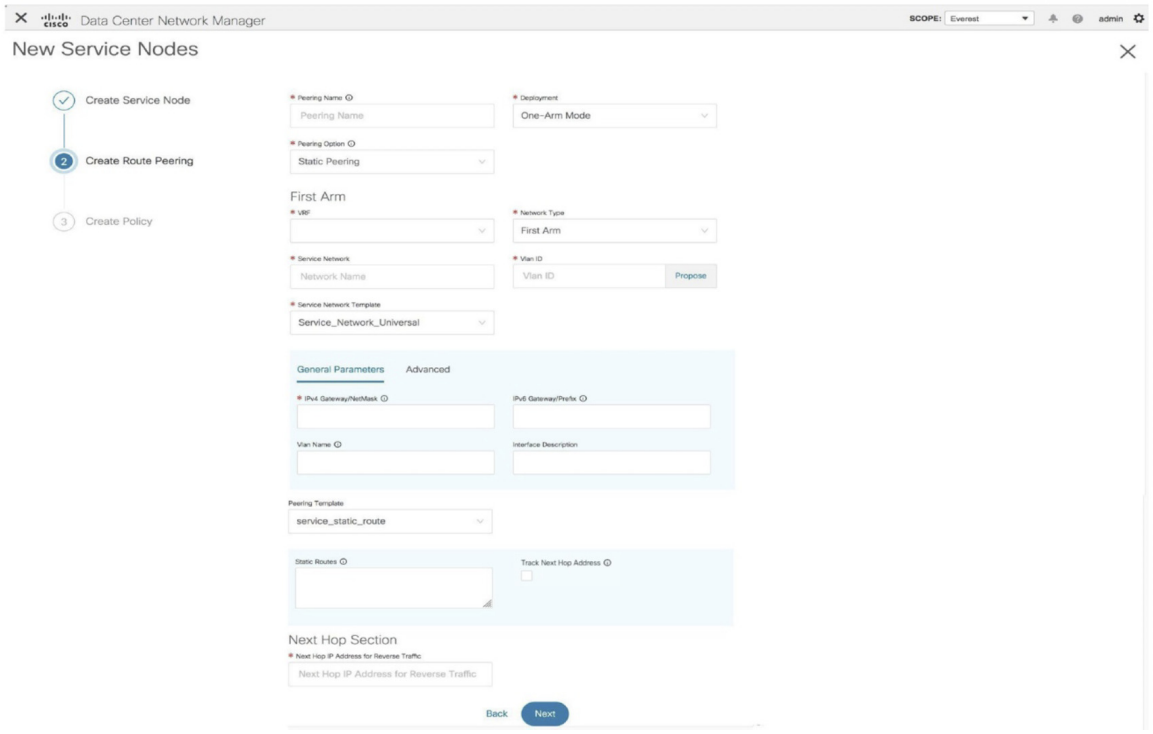
Service Network - Select a service network name from the drop-down list.

Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

Peering Template - Select service_static_route or service_ebgp_route from the drop-down list. For more information on the template fields, refer Templates.

Example: One-Arm Mode Load Balancer



The fields in the **Create Route Peering** window for a One-Arm Mode load balancer deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

Peering Name - Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment - Select One-Arm Mode.

Peering Option - Select Static Peering or eBGP Dynamic Peering.

First Arm

VRF - Select a VRF from the drop-down list..

Network Type - Select First Arm.

Service Network - Select a service network name from the drop-down list.

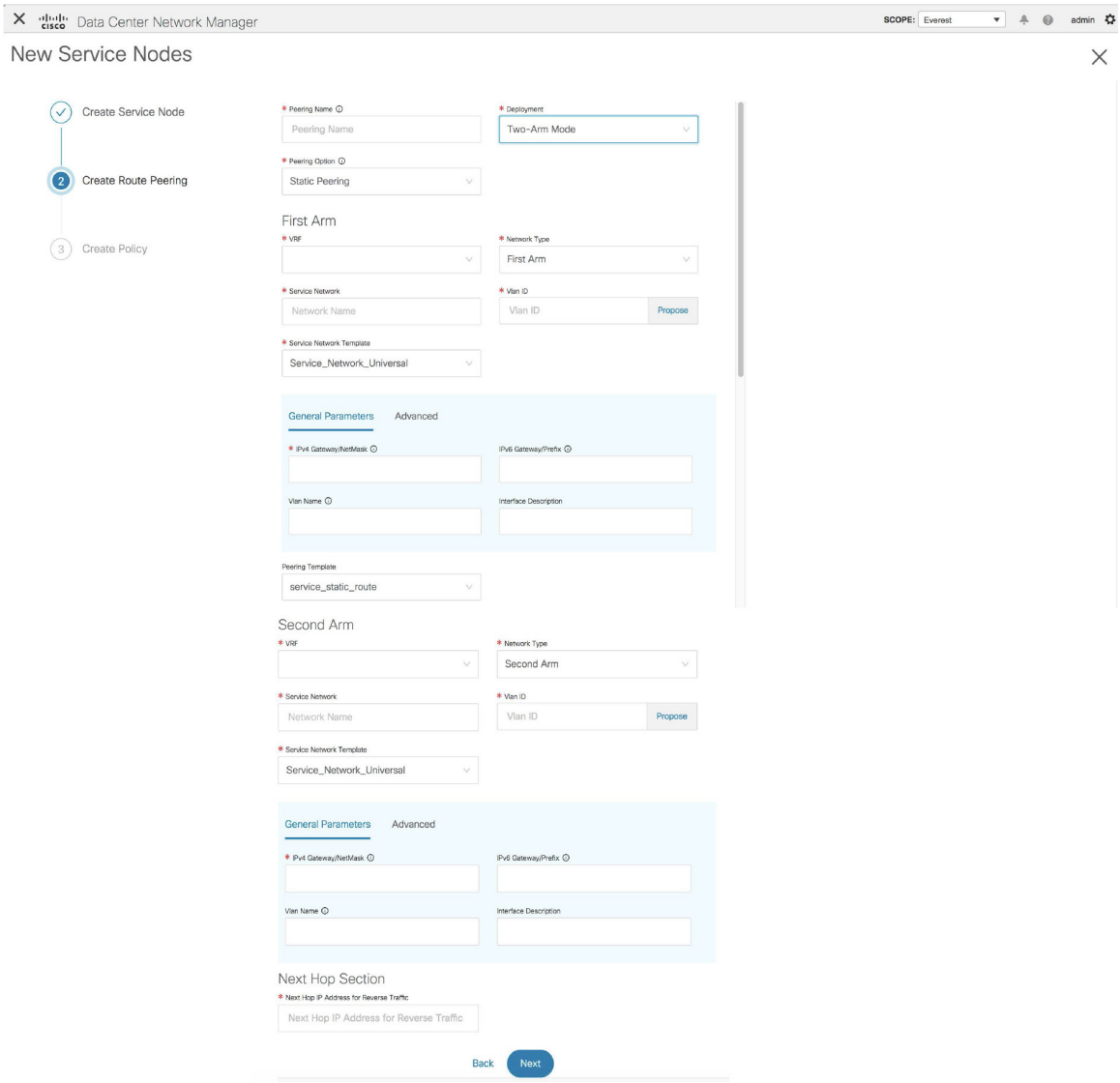
Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

Peering Template - Select service_static_route or service_ebgp_route from the drop-down list. For more information on the template fields, refer Templates.

Next Hop IP Address for Reverse Traffic - Specify the next-hop IP address for reverse traffic.

Example: Two-Arm Mode Load Balancer



The fields in the Create Route Peering window for a Two-Arm Mode load balancer deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

Peering Name - Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment - Select Two-Arm Mode.

Peering Option - Select Static Peering or eBGP Dynamic Peering.

First Arm

VRF - Select a VRF from the drop-down list..

Network Type - Select First Arm.

Service Network - Select a service network name from the drop-down list.

Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

Peering Template - Select service_static_route or service_ebgp_route from the drop-down list. For more information on the template fields, refer Templates.

Second Arm

VRF - Select a VRF from the drop-down list..

Network Type - Select Second Arm.

Service Network - Specify the name of the service network.

Vlan ID - Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined service network VLAN range pool.

Service Network Template - Select the Service_Network_Universal template from the drop-down list. For more information on the template fields, refer Templates.

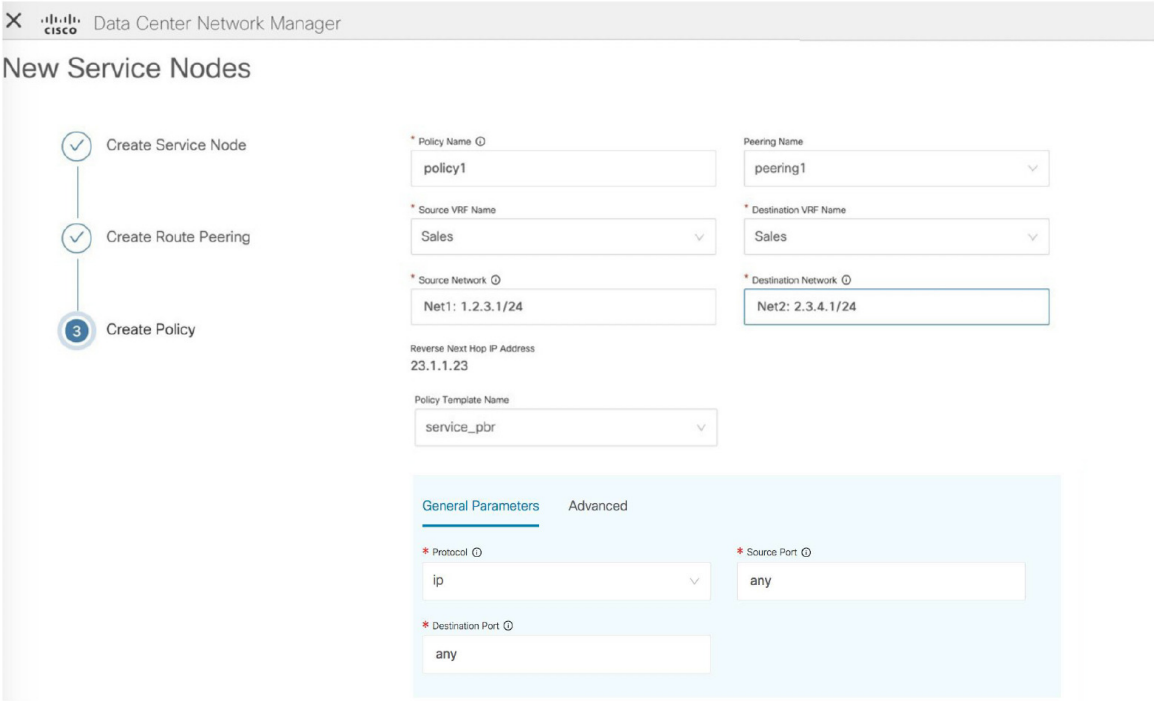
Next Hop Section

Next Hop IP Address for Reverse Traffic - Specify the next-hop IP address for reverse traffic.

Now, click **Next**. The **Create Policy** window is displayed.

Create Service Policy

The **Create Policy** window is displayed as given below.



The fields in the **Create Policy** window are as given below. It is mandatory to fill the fields marked with an asterisk.

Policy Name - Specify a name for the policy.

Peering Name - Select a peering option from the drop-down list.

Source VRF Name - Select a source VRF from the drop-down list.

Destination VRF Name - Select a destination VRF from the drop-down list.

Source Network - Select an IP address from the drop-down list.

Destination Network - Select an IP address from the drop-down list.

Reverse Next Hop IP Address - The reverse next-hop IP address is displayed.

Policy Template Name - Select a template from the drop-down list. For more information on the template fields, refer Templates.

General Parameters

Protocol - Select a protocol from the drop-down list. The options are icmp, ip, tcp, and udp.

Source Port - Specify a source port number. In case the ip protocol is selected, this value is ignored.

Destination Port - Specify a destination port number. In case the ip protocol is selected, this value is ignored.

Starting from Cisco DCNM Release 11.4(1), the **Advanced** tab has been introduced. The options in this tab allow you to customize the matched traffic redirection. For example, you can specify matched traffic to be redirected using PBR, or for matched traffic to bypass a firewall and use routing table rules instead, or you can specify that any matched traffic has to be dropped. You can choose to override the route map match sequence number for prioritization. You can also customize the ACL name, however ensure that the ACL

name that you specify is unique and the same name is not used for another ACL. If you do not specify the route map match sequence number or ACL name, the sequence number will be auto-populated, as in Cisco DCNM Release 11.3(1), from the designated resource pool and the ACL name will be auto-generated based on 5-tuples. For more information on the fields in the **Advanced** tab, refer Templates.

Click **Create**. The service policy is created.

Note Deletion of any service network in Top-Down provisioning that is used by Services is not allowed. Deletion of any regular network that is used in a service policy is also not allowed.

Templates

Service Node Link Templates

service_link_trunk

General Parameters tab

MTU - Specifies the MTU for the interface. By default, this is set to jumbo.

SPEED - Specifies the speed of the interface. By default, this is set to Auto. You can change it to 100Mb, 1Gb, 10GB, 25Gb, 40Gb, or 100Gb, as required.

Trunk Allowed Vlans - Specify 'none',' all' or VLAN ranges. By default, none is specified.

Enable BPDU Guard - Specify an option from the drop-down list. The available options are true, false or no.

Enable Port Type Fast - Select the checkbox to enable spanning tree edge port behavior. By default, this is enabled.

Enable Interface - Uncheck the checkbox to disable the interface. By default, the interface is enabled.

Advanced tab

Source Interface Description - Enter a description for the source interface.

Destination Interface Description - Enter a description for the destination interface.

Source Interface Freeform Config - Enter any addition CLI for the source interface.

Destination Interface Freeform Config - Enter any addition CLI for the destination interface.

service_link_port_channel_trunk

Port Channel Mode - Select a port channel mode from the drop-down list. By default, active is specified.

Enable BPDU Guard - Specify an option from the drop-down list. The available options are true, false or no.

MTU - Specifies the MTU for the interface. By default, this is set to jumbo.

Trunk Allowed Vlans - Specify 'none',' all' or VLAN ranges. By default, none is specified.

Port Channel Description - Enter a description for the port channel.

Freeform Config - Specify the required freeform configuration CLIs.

Enable Port Type Fast - Select the checkbox to enable spanning tree edge port behavior. By default, this is enabled.

Enable Port Channel - Select the checkbox to enable the port channel. By default, this is enabled.

service_link_vpc

This template has no specifiable parameters.

Route Peering Service Network Template

Service_Network_Universal

General Parameters tab

IPv4 Gateway/Netmask - Specify the gateway IP address and mask of the service network.

IPv6 Gateway/Prefix - Specify the gateway IPv6 address and prefix of the service network.

Vlan Name - Specify a name for the VLAN.

Interface Description - Enter a description for the interface

Advanced tab

Routing Tag - Specify a routing tag. Valid values range from 0 to 4294967295.

Route Peering Templates

service_static_route

Enter the static routes in the **Static Routes** field. You can enter one static route per line.

service_ebgp_route

General Parameters tab

Neighbor IPv4 - Specify the IPv4 address of the neighbor.

Loopback IP - Specify the IP address of the loopback.

Advanced tab

Neighbor IPv6 - Specify the IPv6 address of the neighbor.

Loopback IPv6 - Specify the IPv6 address of the loopback.

Route-Map TAG - Specify route-map tag that is associated with the interface ID.

Interface Description - Enter a description for the interface.

Local ASN - Specify a local ASN to override the system ASN.

Advertise Host Routes - Select the checkbox to enable advertisement of /32 and /128 routes to edge routers.

Enable Interface - Uncheck the checkbox to disable the interface. By default, the interface is enabled.

Service Policy Template

service_pbr

General Parameters tab

Protocol - Select a protocol from the drop-down list. The options are icmp, ip, tcp, and udp.

Source port - Specify a source port number. In case the ip protocol is selected, this value is ignored.

Destination port - Specify a destination port number. In case the ip protocol is selected, this value is ignored.

Advanced tab

Route Map Action - Select an action from the drop-down list. The options are permit or deny. If you select **permit**, the matched traffic is redirected based on the next-hop option and the defined policy. If you select **deny**, the traffic is routed based on the routing table rules.

Next Hop Option - Specify an option for the next-hop. The options are **none**, **drop-on-fail**, and **drop**.If you select **none**, the matched traffic is redirected based on the defined PBR rules. If you select **drop-on-fail**, the matched traffic is dropped if the specified next hop is not reachable. If you select **drop**, the matched traffic is dropped.

ACL Name - Specify a name for the generated access control list (ACL). If not specified, this is auto-generated.

ACL Name for reversed traffic - Specify a name for the ACL that is generated for reversed traffic. If not specified, this is auto-generated.

Route map match number - Specify a route map match number. A valid value ranges from 1 to 65535. If not specified, a route map match sequence number will be retrieved from the predefined resource pool. This number is associated with the name of the ACL.

Route map match number for reversed traffic - Specify a route map match number for reversed traffic. A valid value ranges from 1 to 65535. If not specified, a route map match sequence number will be retrieved from the predefined resource pool. This number is associated with the name of the ACL that has been generated for reversed traffic.

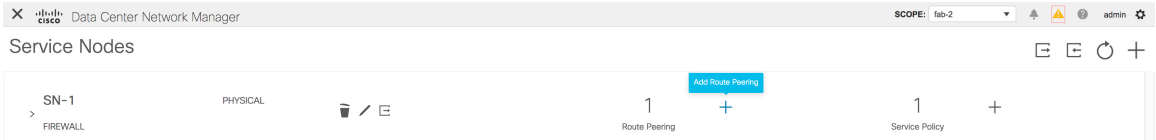
You can also customize the templates based on specific requirements. For more information on templates, refer Template Library.

Adding a Route Peering

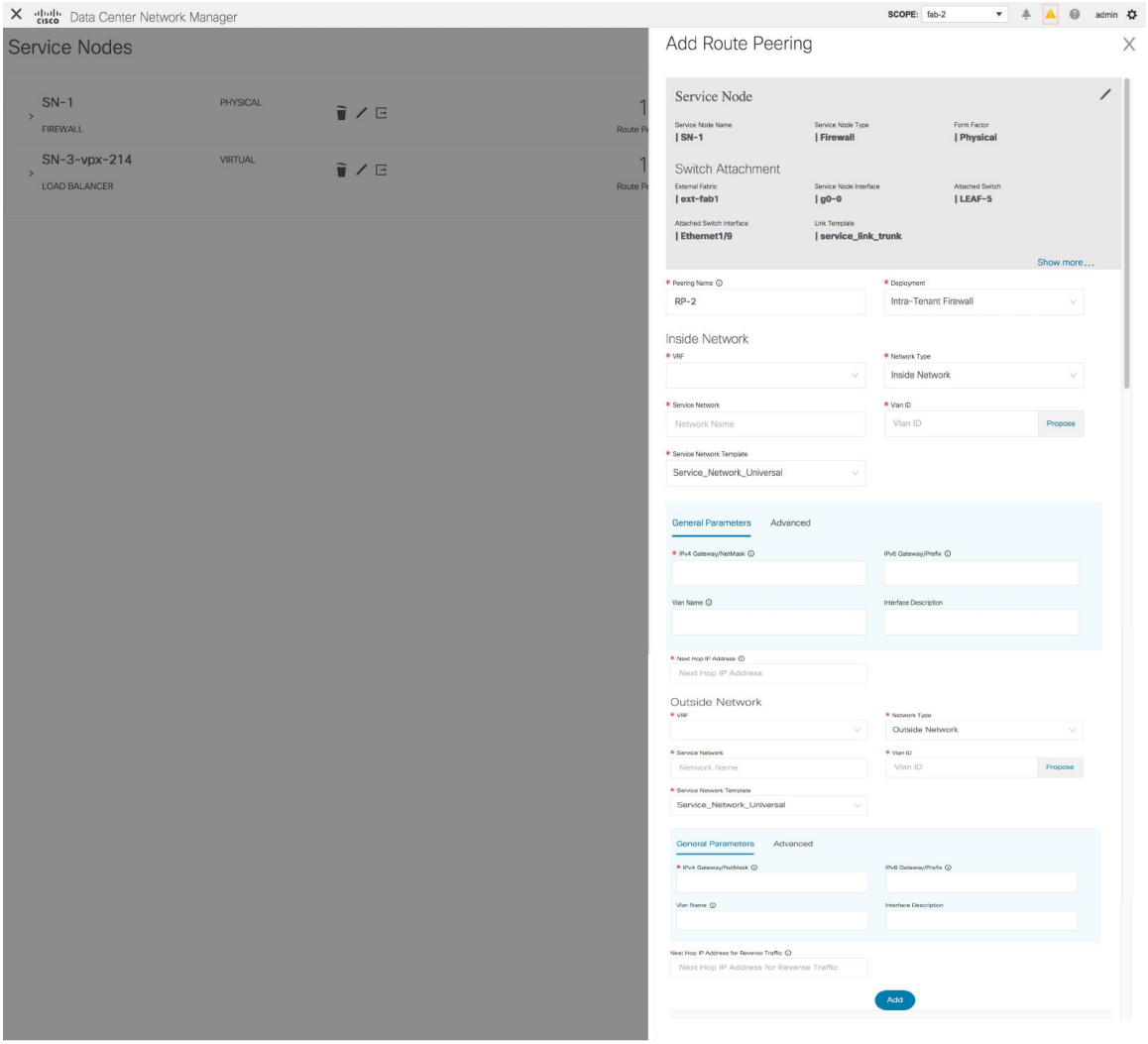
To add a route peering from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Click the **Add Route Peering** icon on the **Service Nodes** window.



Step 2 The **Add Route Peering** window is displayed.



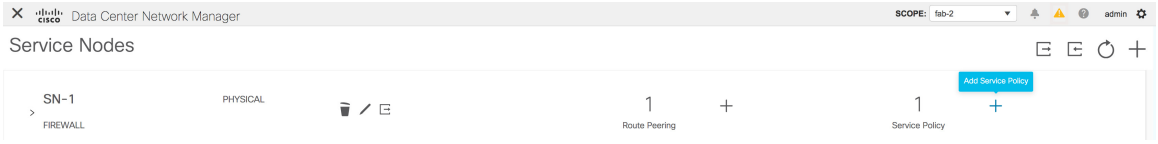
Specify the required parameters and click **Add**. For more information on specific fields, hover over the **i** icon.

Adding a Service Policy

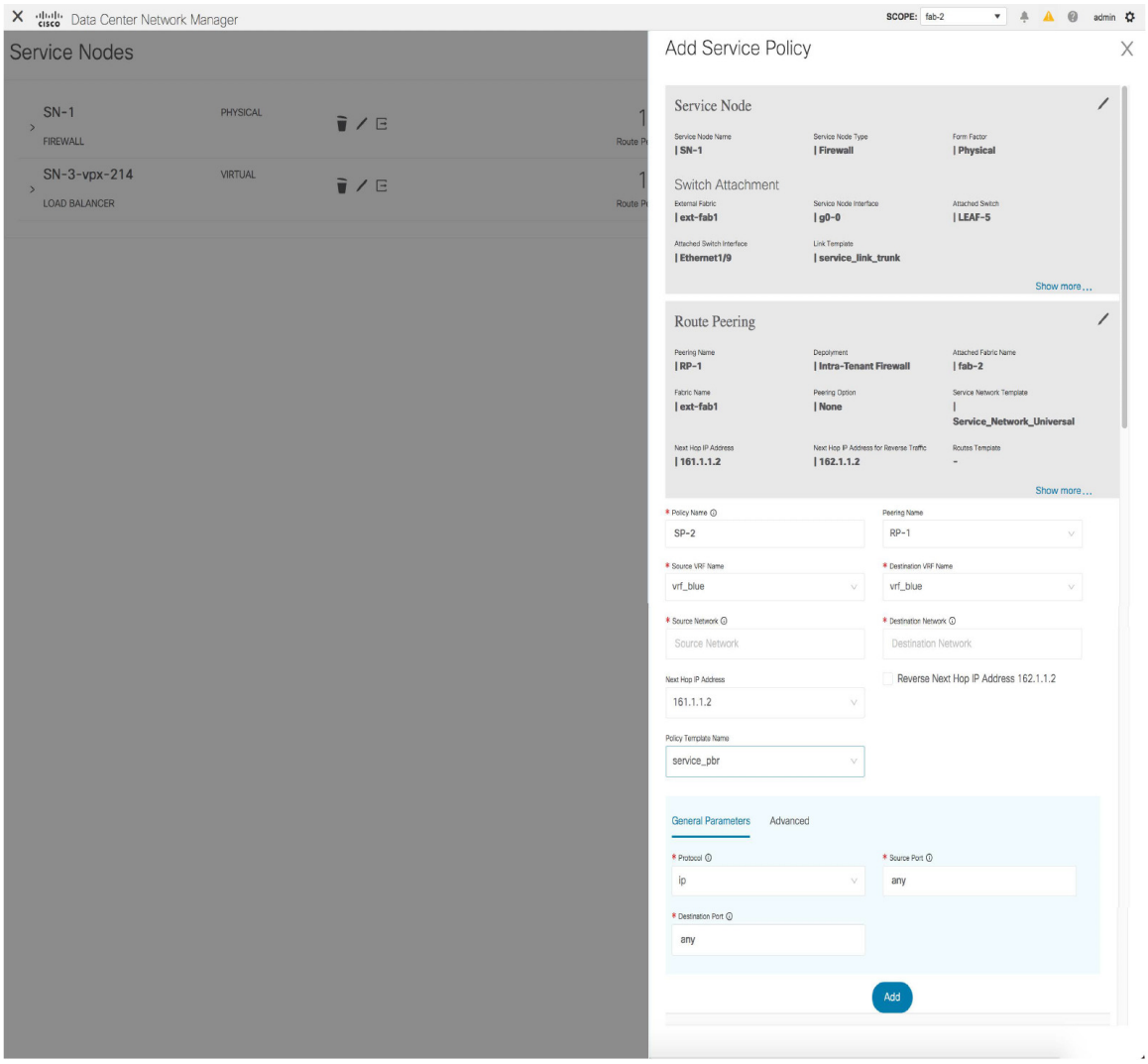
To add a service policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Click the **Add Service Policy** icon on the **Service Nodes** window.



Step 2 The **Add Service Policy** window is displayed.



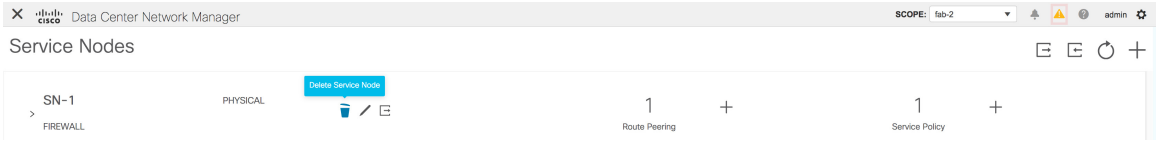
Specify the required parameters and click **Add**. For more information on specific fields, hover over the **i** icon.

Deleting a Service Node

To delete a service node from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Click the **Delete Service Node** icon on the **Service Nodes** window.



Step 2 A pop-up window comes up to confirm if the node has to be deleted. Click **Delete**.

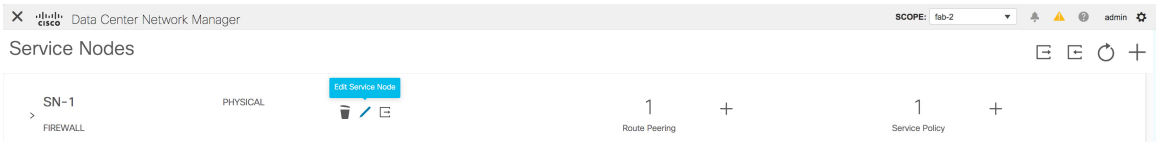
Note Ensure that the service node that has to be deleted has no route peering or service policies associated with it. In case there are service policies or route peering associated with the service node, the deletion is blocked with a warning indicating that any route peering or service policies associated with the service node have to be removed before deleting the service node.

Editing a Service Node

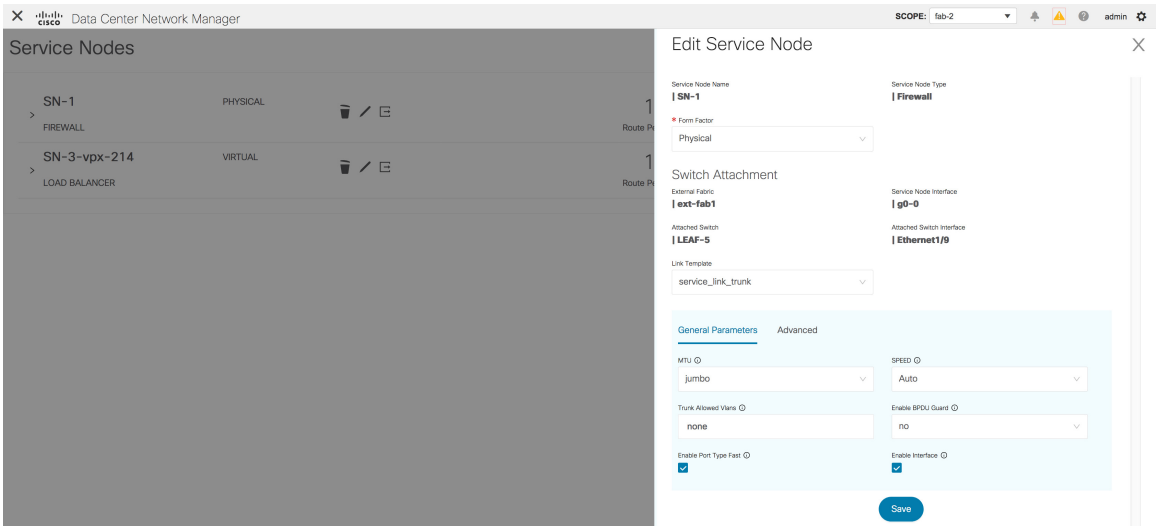
To edit a service node from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Click the **Edit Service Node** icon on the **Service Nodes** window.



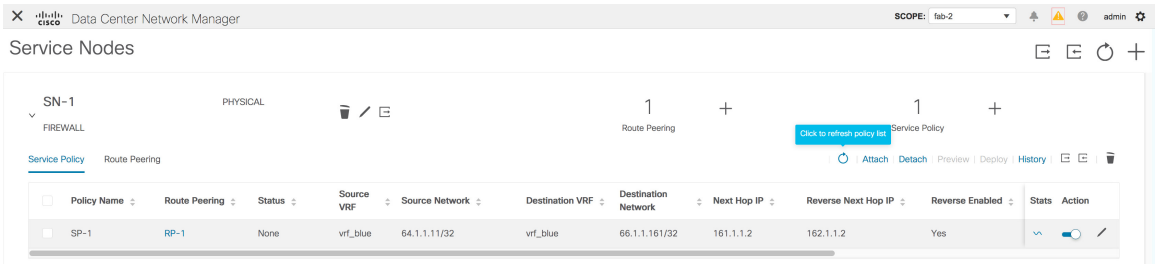
Step 2 The **Edit Service Node** window is displayed.



Make the required changes and click **Save**.

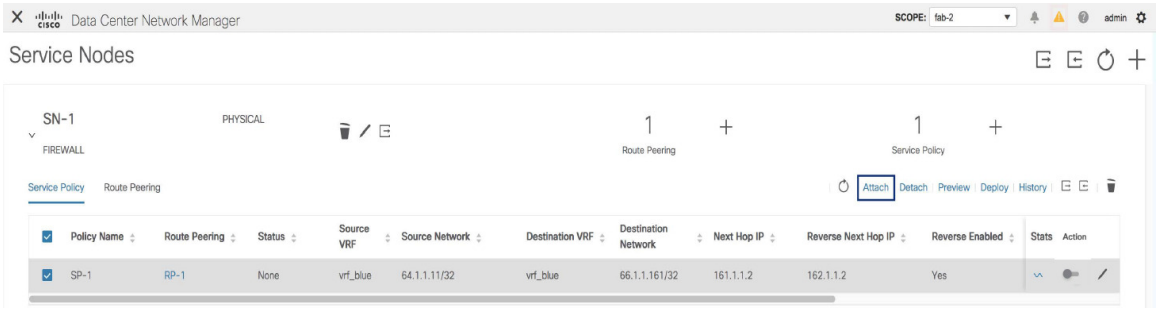
Refreshing the Service Policy and Route Peering List

To refresh the list of service policies or route peerings that is displayed in the **Service Nodes** window, click the **Refresh** icon that appears in the **Service Policy** tab or the **Route Peering** tab.



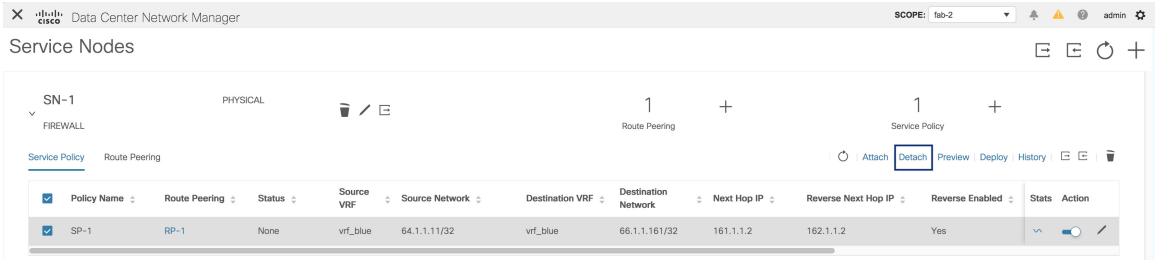
Attaching a Service Policy or a Route Peering

To attach a specific service policy or route peering from a switch, select the checkbox next to the required service policy or route peering and click **Attach**.



Detaching a Service Policy or a Route Peering

To detach a specific service policy or route peering from a switch, select the checkbox next to the required service policy or route peering and click **Detach**.

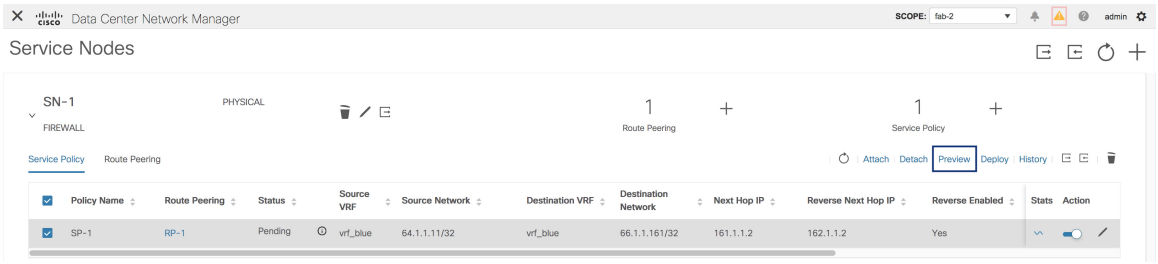


Preview a Service Policy or a Route Peering

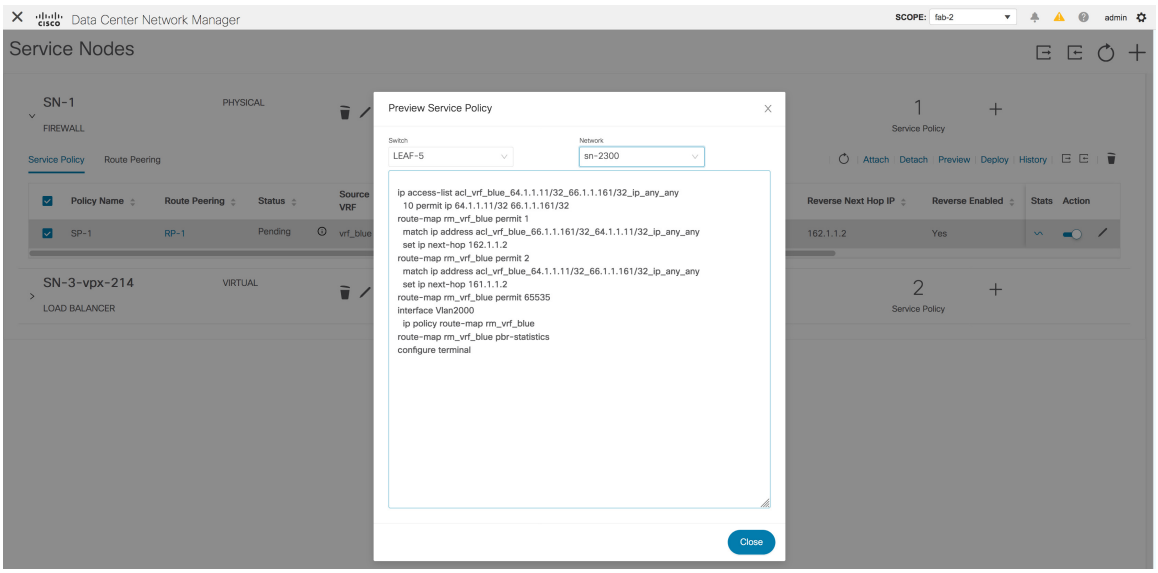
To display the preview of a service policy or a route peering from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Select a service policy or route peering checkbox and click **Preview** on the **Service Nodes** window.



A **Preview Service Policy** or a **Preview Route Peering** window is displayed.



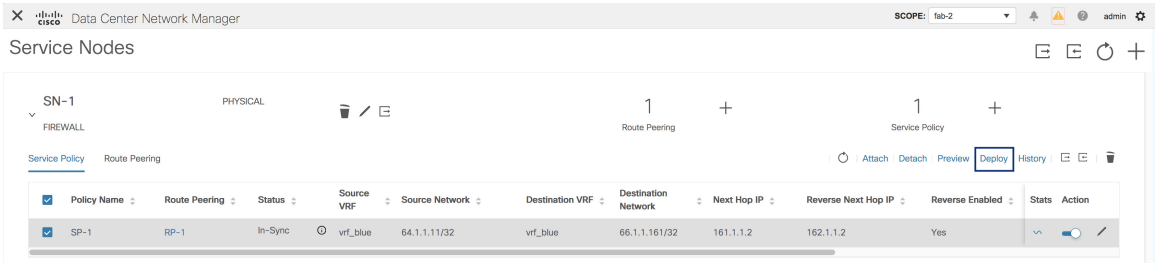
Step 2 Select a specific switch or network from the respective drop-down lists to display the service policies or route peerings for specific switches and networks. Click **Close** to close the window.

Deploying a Service Policy or a Route Peering

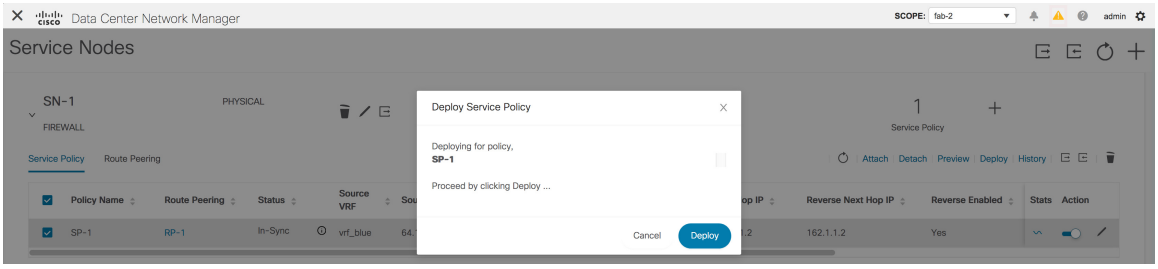
To deploy a service policy or a route peering from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Select a service policy or route peering checkbox and click **Deploy** on the **Service Nodes** window.



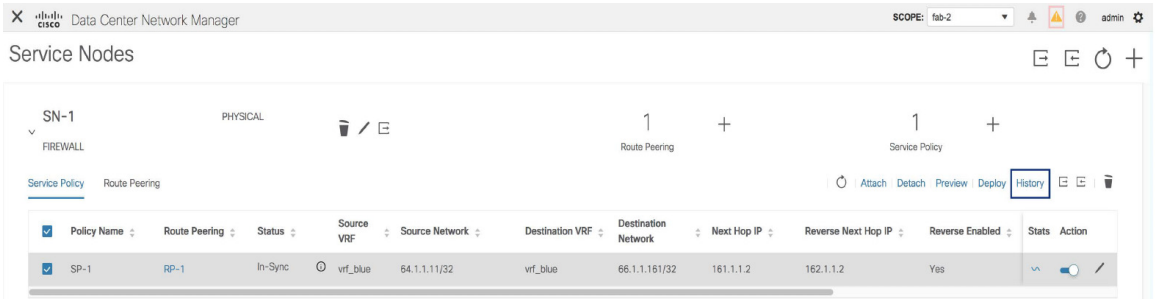
A pop-up window is displayed asking for confirmation to deploy.



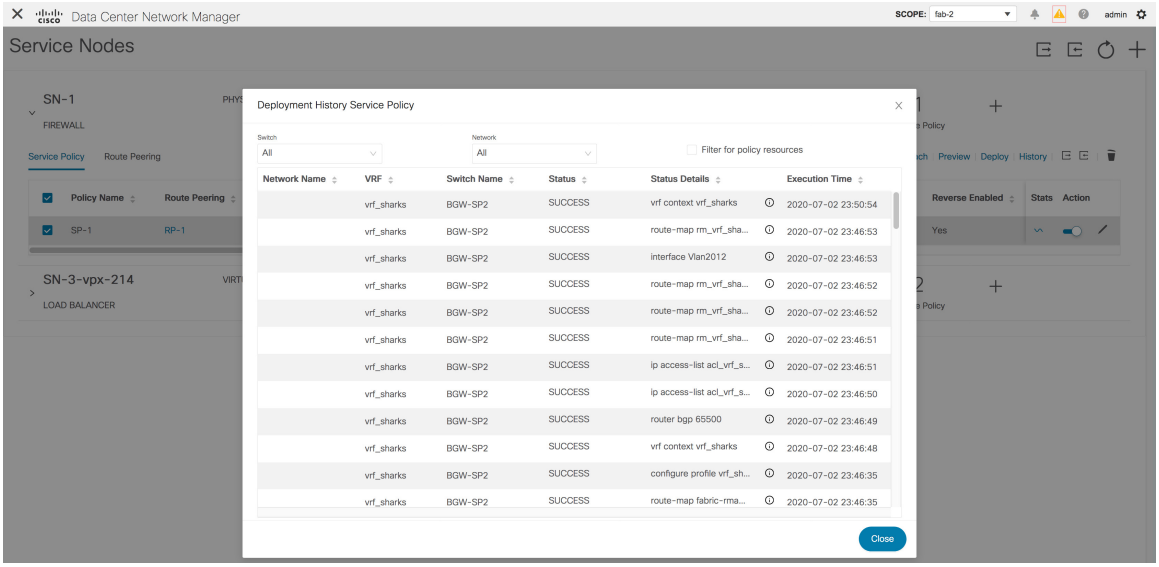
Step 2 Click **Deploy**.

Viewing Deployment History

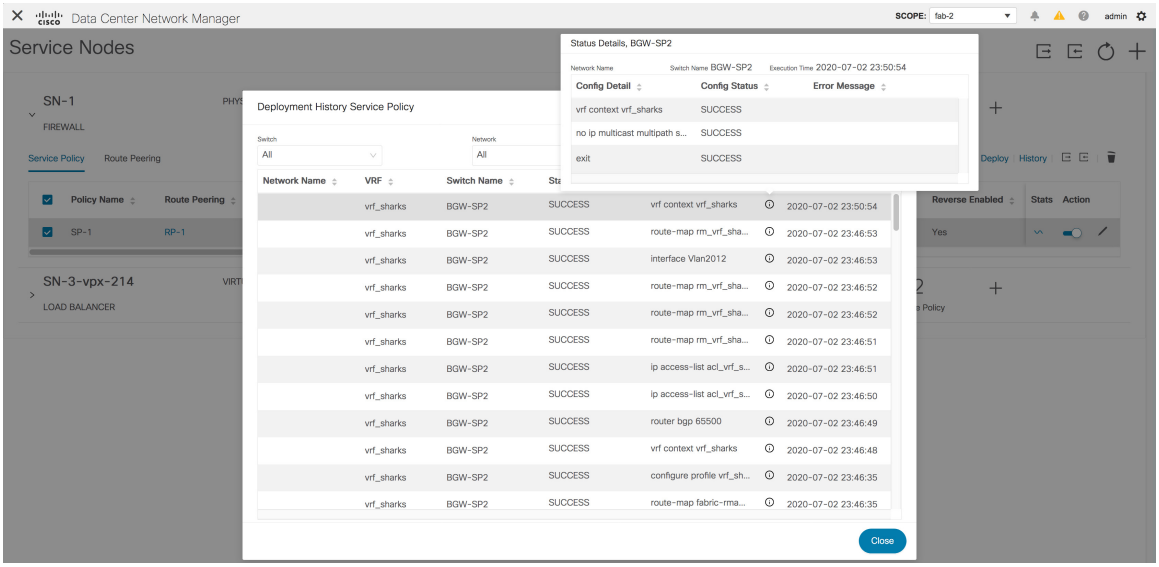
To view deployment history of the switches and networks that are involved in the selected service policy or route peering, click **History** in the **Service Policy** tab or the **Route Peering** tab. The **Deployment History Service Policy** or the **Deployment History Route Peering** window is displayed.



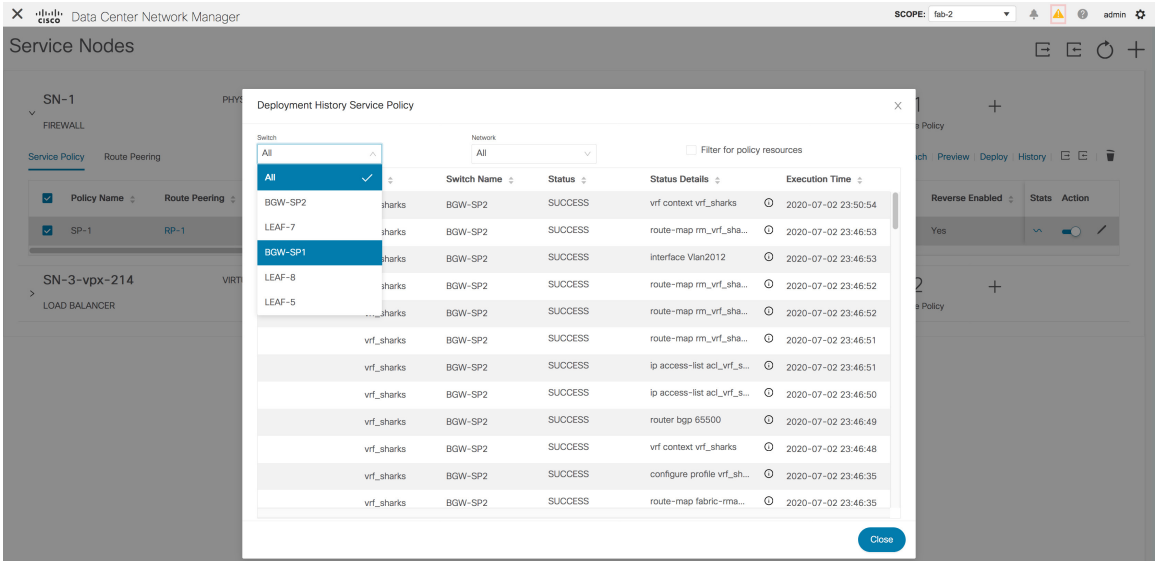
Information such as the name of the network, VRF, and switch, status, status details, and time of execution is displayed.



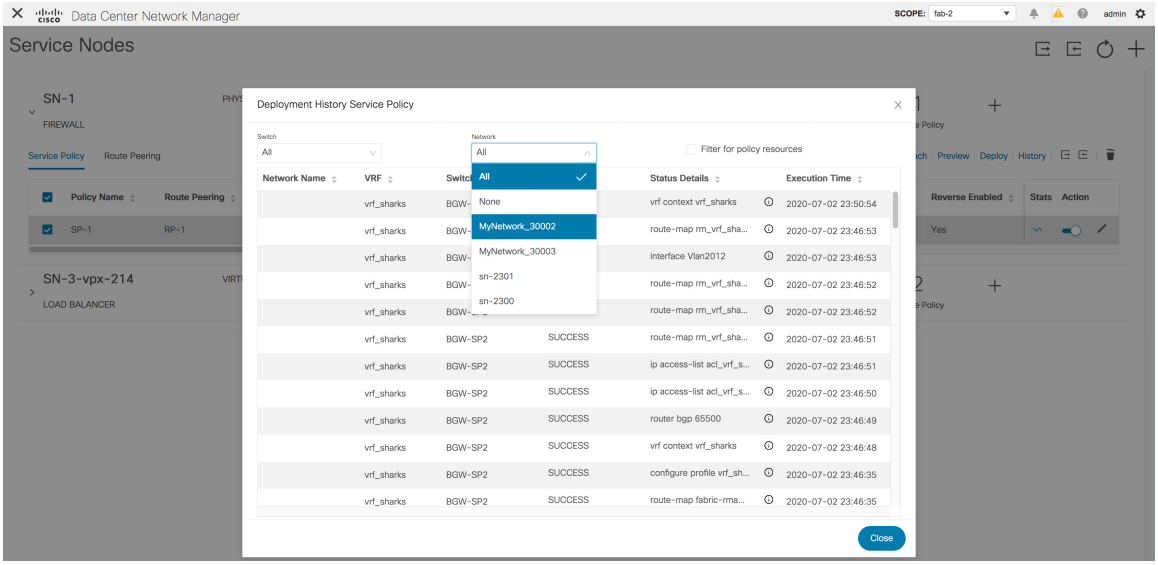
The first line in the list of CLIs is displayed in the **Status Details** column. This provides a peak into the deployed configuration. Hover over the **i** icon next to the **Status Details** field in each row to display more information.



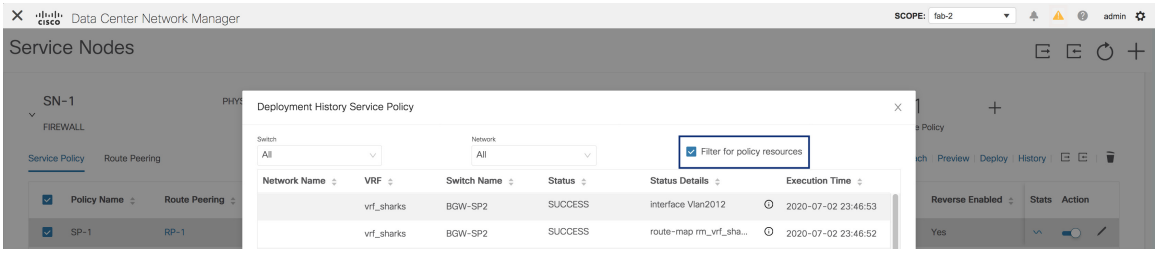
Select a switch from the **Switch** dropdown list to display information for the selected switch.



Select a network from the **Network** dropdown list to display information for the selected network.

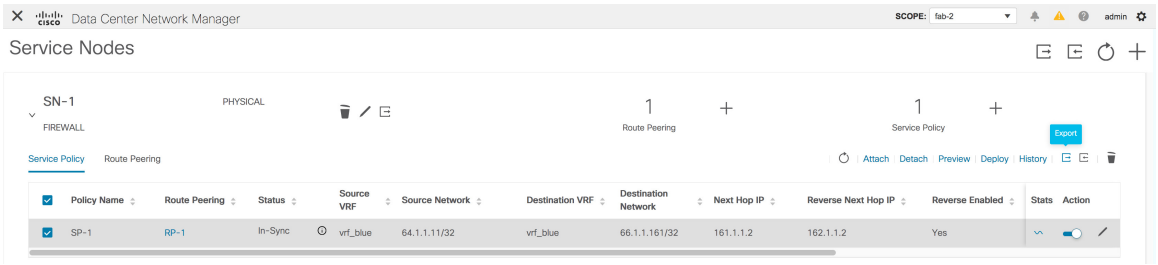


Select the **Filter for policy resources** checkbox to display only policy-related deployments such as ACLs, route maps and associated CLIs. This checkbox is available only in the **Deployment History Service Policy** window.



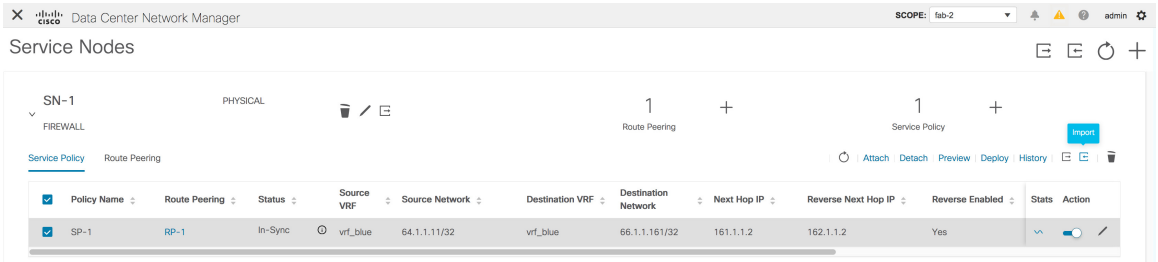
Exporting a Service Policy or a Route Peering Table

To export the service policy or route peering information as an Excel file, click the **Export** icon on the **Service Nodes** window. Click the **Export** icon on the **Service Policy** tab to export information about the service policies. Click the **Export** icon on the **Route Peering** tab to export information about the route peerings.



Importing a Service Policy or a Route Peering Table

To import service policy or route peering information as an Excel file, click the **Import** icon on the **Service Nodes** window. Click the **Import** icon on the **Service Policy** tab to export information about the service policies. Click the **Import** icon on the **Route Peering** tab to export information about the route peerings.

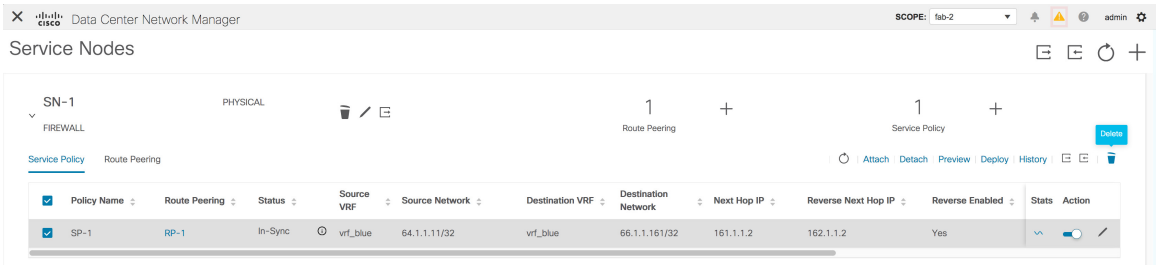


Deleting a Service Policy

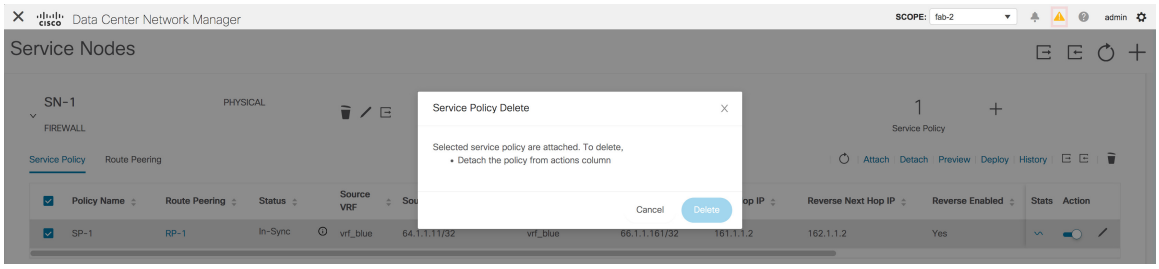
To delete a service policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Select the service policy that has to be deleted by clicking the checkbox that is next to the name of the policy, and then click the **Delete** icon on the **Service Nodes** window.



Step 2 A pop-up window is displayed asking for confirmation to delete. Click **Delete**. In case the service policy that has to be deleted is attached, the pop-up window indicates that the service policy has to be detached by using the toggle in the **Action** column, and deploying the changes (removing the policy) before it can be deleted.

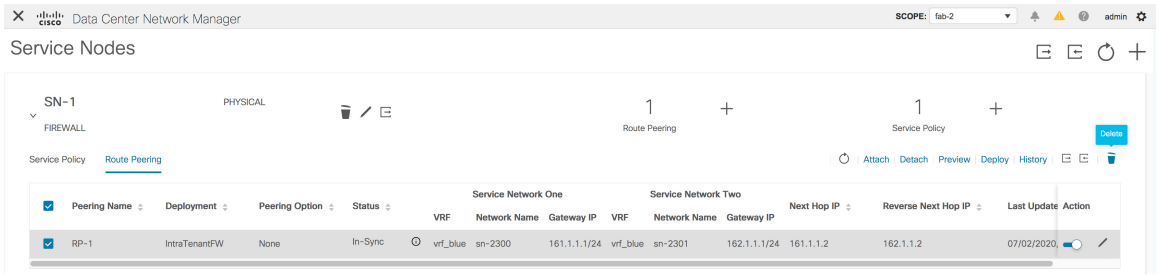


Deleting a Route Peering

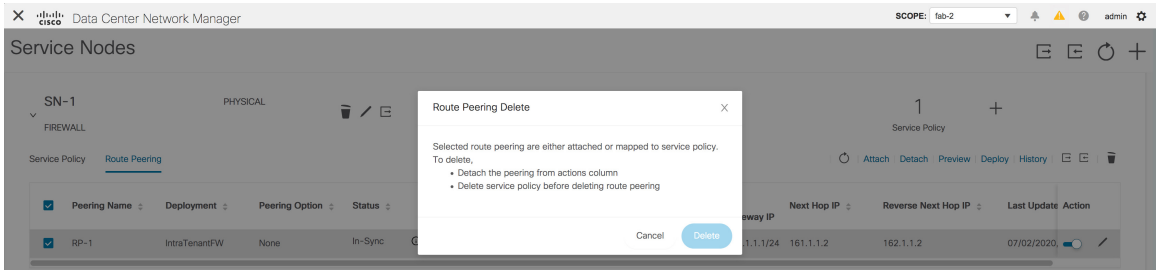
To delete a route peering from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Select the route peering that has to be deleted by clicking the checkbox that is next to the name of the route peering, and then click the **Delete** icon on the **Service Nodes** window.



Step 2 A pop-up window is displayed asking for confirmation to delete. Click **Delete**. In case the route peering that has to be deleted is attached or if the service policy associated with the route peering is active, the pop-up window indicates that the peering has to be detached by using the toggle in the **Action** column, deploy the changes (remove the policy), and delete the service policy associated with the route peering before the route peering can be deleted.



Viewing Service Policy Information

In the **Service Nodes** window, the **Service Policy** tab displays information about the configured service policies.

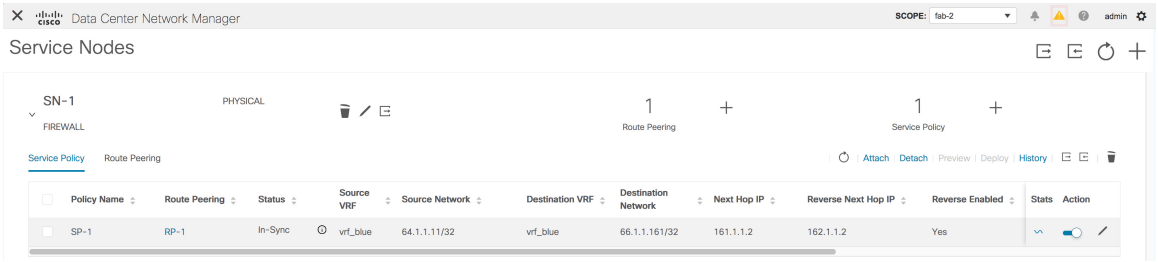
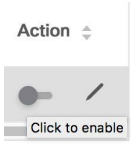


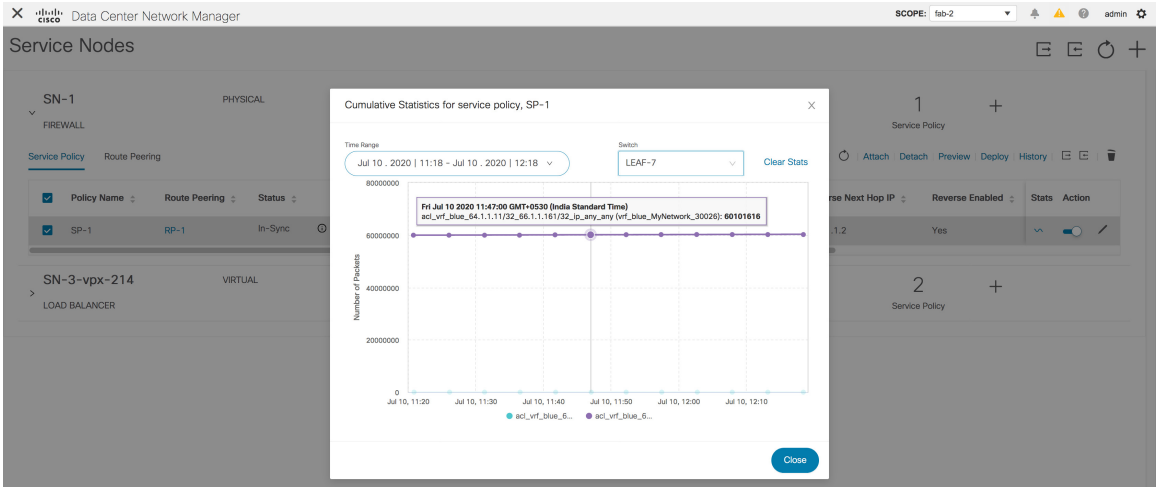
Table 1: Service Policy Table Field and Description

Field	Description
Policy Name	Displays the name of the policy.
Route Peering	Displays the route peering name given for the peering configuration. Click the specified peering name to display route peering information.
Status	Displays the status of the service policy.
Source VRF	Displays the Virtual Routing and Forwarding (VRF) source.
Source Network	Displays the source network.
Destination VRF	Displays the destination VRF.
Destination Network	Displays the destination network.
Next Hop IP	Displays the next-hop IP address.
Reverse Next Hop IP	Displays the reverse next-hop IP address.
Reverse Enabled	Displays if reverse next-hop is enabled or not.
Route Map Action	Displays the specified route map action.
Next Hop Option	Displays the specified next hop option.
Last Updated	Displays the time at which the service policy was last updated.
Stats	Click the graph line to display cumulative statistics for a policy in a specified time range. For more information, refer Stats.

Field	Description
Action	Use the toggle to enable/attach or disable/detach the service policy. When the service policy is attached or enabled, the corresponding policies are applied to the VRF (tenant), source, and destination networks.  The toggle turns blue in color when the service policy is attached or enabled. Click the **Edit** icon to edit the service policy.

Stats

In the **Service Nodes** window, the **Service Policy** tab displays statistical information about the configured service policies. Select a time range for which the statistics should be displayed from the **Time Range** drop-down box. You can select the date from the calendar displayed on the window and the time by clicking **select time** at the bottom right corner of the window. You can also display statistics from the last 15 minutes, 1 hour, 6 hours, 1 day, and 1 week. Select the required time range and click **Apply**. Select a switch for which the statistics should be displayed from the **Switch** drop-down list. The statistics are then displayed for the selected switch in the specified time range. Starting from Cisco DCNM Release 11.4(1), you can click **Clear Stats** to reset the statistics for a specific policy on all involved switches. If multiple policies are sharing the same route map, then the statistics of other policies are also impacted.



Viewing Route Peering Information

In the **Service Nodes** window, click **Route Peering**. The **Route Peering** tab displays route peering information.

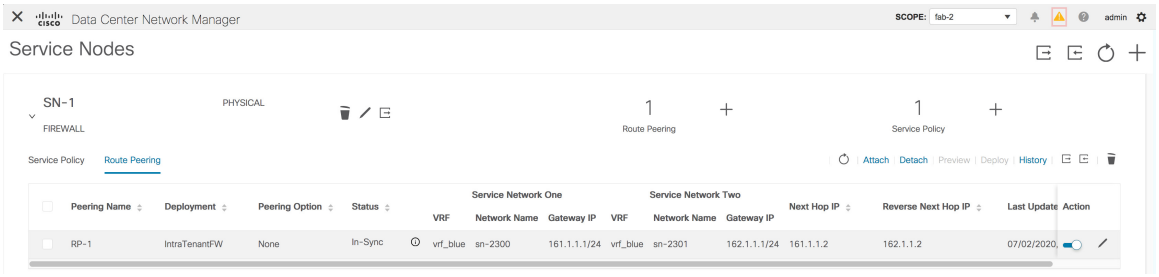
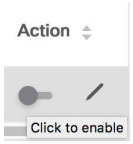
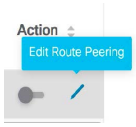


Table 2: Route Peering Table Field and Description

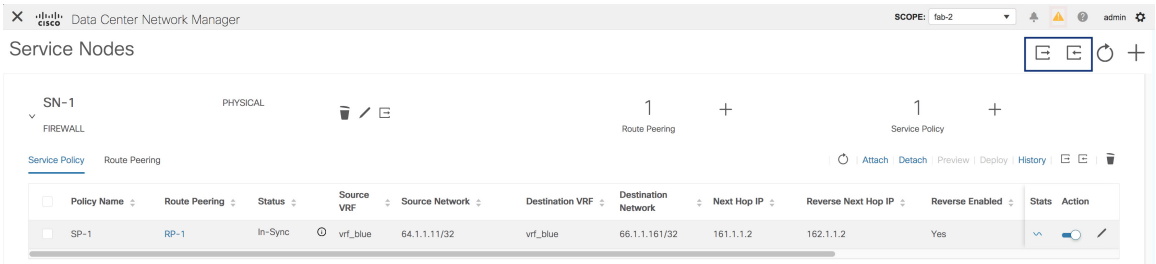
Field	Description
Peering Name	Displays the defined peering name.
Deployment	Displays the deployment - One-Arm mode or Two-Arm mode.
Peering Option	Displays the peering option - Static or eBGP Dynamic peering.
Status	Displays the status of the route peering.
Service Network VRF	Displays the service network VRF.
Service Network Name	Displays the name of the service network.
Service Network Gateway IP	Displays the gateway IP of the service network VRF.
Next Hop IP	Displays the next-hop IP address.
Reverse Next Hop IP	Displays the reverse next-hop IP address.

Field	Description
Last Updated	Displays the time at which the route peering was last updated.
Action	Use the toggle to enable/attach or disable/detach the route peering. When the route peering is enabled, the service networks defined in that route peering will be attached to the service leaf.  The toggle turns blue in color when the route peering is attached or enabled. Click the **Edit** icon to edit the route peering. 

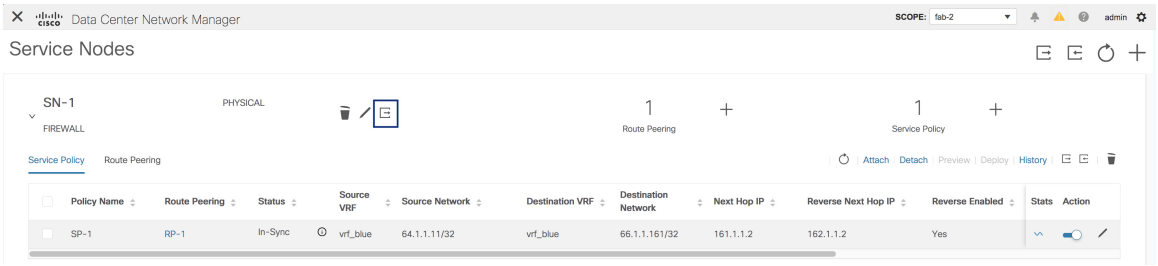
Service Node Backup and Restore

You can back up data at the service node level by clicking the **Export** icon to export data about the service nodes to an excel file. Data regarding all the service nodes, the respective route peerings and service policy, is exported.

You can also restore the service node level data by clicking the **Import** icon to import data about the service nodes from an excel file.



You can also export data for a specific service node by clicking the **Export** icon located next to the **Edit Service Node** icon.



Fabric Backup and Restore

During easy fabric and parent MSD fabric backup, the service node connections, route peering and service policy configurations, such as composed ACL and route-map, are saved as part of the fabric, VRF and the tenant network intent. However, the definitions of service node, route peering and service policy are not saved. We recommend backing up the service data by clicking the **Export** icon at the service node level from the **Control > Services** window. While restoring easy fabrics and parent MSD fabrics, the service data can be restored by clicking the **Import** icon at the service node level from the **Control > Services** window. The service node connections, route peering and service policy configuration will be restored along with the associated fabric, VRF and the tenant network intent.

Brownfield Migration

During brownfield migration, the L4-L7 service configuration, such as ACLs and route-maps associated with networks and VRFs, are captured in the switch freeform policy linked to the tenant network and the VRF profile. No service node, route peering, or service policy is auto-generated as a result of brownfield migration. If you want to apply a new service policy to the same tenant network or VRF, remove the captured freeform configuration and configuration compliance will then generate the required CLIs that you can deploy later.